

Journal of Technology Law & Policy

Volume 23

Number 1

ARTICLES

INTELLECTUAL CONTRACT AND INTELLECTUAL
LAW

Daniel F. Spulber 1

THE CALIFORNIA CONSUMER PRIVACY ACT:
TOWARDS A EUROPEAN-STYLE
PRIVACY REGIME IN THE
UNITED STATES?

Stuart L. Pardau 68

BENEFIT OF THE BUT-FOR BARGAIN: ASSESSING
ECONOMIC TOOLS FOR DATA PRIVACY
LITIGATION

Mike Kheyfets 115

CHILD PRIVACY IN THE DIGITAL AGE AND
CALIFORNIA'S CHILD DELETION
STATUTE

Michael Shepherd 134

EDITORIAL BOARD

2018–2019

EDITOR IN CHIEF
Rebekah Allison

ASSISTANT EDITORS IN CHIEF
Aaron Crews
Brendan Collins

EXECUTIVE EDITOR IN RESIDENCE
Adam J. Duso

EXECUTIVE MANAGING EDITOR
Ashley Genoese

EXECUTIVE ARTICLES EDITOR
Justin Shifrin

EXECUTIVE STUDENT WORKS
EDITOR
Ellyse Collins

EXECUTIVE RESEARCH EDITOR
Shannon Anderson

EXECUTIVE GALLEYS EDITOR
Michael Liles

EXECUTIVE COMMUNICATIONS
EDITOR
Patrick Salmon

GENERAL BOARD

2018–2019

Farhaan Anjum
Andrew Bayudan
Avigail Bacharach
Alexandra Beguiristain
Tyra Carroll
Jacob Cohen
Elpidio Cruz
Melissa Dangond
James Dority
Jacob Duval
Kimano Edwards
Michael Farhat
William Ford
Michael Friedman
Mendel Harlig
John Harper
Laura Hendee
Geneva Hernandez
Matthew Hutchisson
Andrew Ingber
Ian Johnson
Jessey Krehl

Brett Lashley
Carlos Lievano
Gabriella Morillo
Abraham Oxner
Esther Oyetoro
Gabriel Pla
Stephanie Pocatko
Jacob Post
Ty Pryor
Richard Russo
John Rutledge
Eleanor Samuels
Alfredo Sarduy
Matthew Sawyer
Michael Shepherd
Justin Shifrin
Brandon Singh
Lana Smith
Mariya Solomiy
Bradley Spivey
Kyle Swanson
Luke Tobis
Richard Windisch

FACULTY ADVISOR
Stacey Steinberg

STAFF EDITOR
Lisa Caldwell

INTELLECTUAL CONTRACT AND INTELLECTUAL LAW

*Daniel F. Spulber**

Abstract

Technological change is altering the nature of contract toward a greater focus on intangible assets. The direction of technological change toward greater connectivity, interoperability, mobile communications, the Internet of Things (IoT), artificial intelligence (AI), virtual inventions, and cooperative research and development (R&D) has profound implications. This Article develops a new framework that I refer to as “Intellectual Law” to address this shift. It will introduce the new concept of “Intellectual Contract” (IC) to characterize an agreement for invention, innovation, and technology adoption. This Article also introduces the concept of “Intellectual Tort” (IT) to describe liability including but not limited to misappropriation of trade secrets and infringement of patents, trademarks, and copyrights. Intellectual Law provides a consistent framework for IC, IT and Intellectual Property (IP). The article observes that legal protections for inventors cannot rely solely on what has proven to be a flawed combination of IT and IP. This Article argues that greater emphasis on IC rules would improve both IT and IP. Because an IC protects expectation interests, it is essential for creating, developing, sharing, and applying intangible assets. An IC generates gains from trade that enhance the benefits of inventors, innovators and adopters beyond what can be achieved by IT and IP alone. The discussion sets forth some broad principles for IC law, examines the differences between an IC and a standard contract, and identifies the main forms of ICs.

INTRODUCTION	2
I. INTELLECTUAL LAW	10
A. <i>The Conflict Between IT and IP</i>	10
B. <i>Untangling IT and IP</i>	15
C. <i>ICs and the “Market for Innovative Control”</i>	17
D. <i>ICs and the Nature of the Firm</i>	27

* Elinor Hobbs Distinguished Professor of International Business and Professor of Strategy, Strategy Department, Kellogg School of Management, Northwestern University, 2211 Campus Drive, Evanston, IL, 60208; Professor of Law (Courtesy), Pritzker School of Law, Northwestern University. E-mail: jems@kellogg.northwestern.edu. I gratefully acknowledge research support from Qualcomm and the Kellogg School of Management. I thank Alexei Alexandrov, Robert Merges, Ivan Png, Danny Sokol, and Andrew Toole for their helpful comments on an earlier draft. I also thank participants at the Eleventh Annual Searle Center/USPTO Conference on Innovation Economics, June 21–22, 2018, Northwestern University Pritzker School of Law.

II.	INTELLECTUAL CONTRACT	31
A.	<i>ICs and Incompleteness of IP</i>	31
B.	<i>ICs and Excludability of IP</i>	37
C.	<i>ICs and Non-Rivalrous Usage of IP</i>	41
D.	<i>ICs and Incentives for Exploratory Performance</i>	42
E.	<i>ICs and Fundamental Uncertainty</i>	47
III.	INTELLECTUAL CONTRACT TYPES	53
A.	<i>Employment Contracts</i>	53
B.	<i>Outsourcing Contracts</i>	57
C.	<i>Joint Venture and Consortium Contracts</i>	59
D.	<i>License Contracts</i>	61
E.	<i>Platform Contracts</i>	64
	CONCLUSION	67

INTRODUCTION

Conceptual legal frameworks must catch up with fundamental technological change. Major technological developments include dramatic increases in digital connectivity and interoperability as well as significant advances in Information and Communications Technology (ICT).¹ These technological shifts drive what has been called the Fourth Industrial Revolution (4IR).² Important innovations that involve digital connectivity and interoperability include the Internet of Things (IoT), artificial intelligence (AI), cloud computing, data analytics, mobile communications, autonomous vehicles, additive manufacturing, and virtual reality.³

1. YANN MÉNIÈRE ET AL., EUROPEAN PATENT OFFICE, PATENTS AND THE FOURTH INDUSTRIAL REVOLUTION: THE INVENTIONS BEHIND DIGITAL TRANSFORMATION 17 (European Patent Office ed., 2017) (“[T]he combined use of a wide range of new technologies in a large variety of sectors of the economy. These include digitisation and highly effective connectivity, but also technologies such as cloud computing and artificial intelligence that have permitted the development of interconnected smart objects operating autonomously.”).

2. Klaus Schwab, *The Fourth Industrial Revolution: What It Means and How to Respond*, FOREIGN AFFAIRS (Dec. 12, 2015), <https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution> (“The First Industrial Revolution used water and steam power to mechanize production. The Second used electric power to create mass production. The Third used electronics and information technology to automate production. Now a Fourth Industrial Revolution is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.”); see also KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION (2017).

3. See MÉNIÈRE, *supra* note 1, at 17–18.

Achieving digital connectivity involves the formation of networks with many companies providing network components and connecting devices to the network, including mobile communications and autonomous vehicles. Companies require contracts to coordinate digital connectivity. As Spulber and Yoo observe, “networks come from supply decisions by network providers, interconnection between networks, demand decisions by network customers, and supply decisions by providers of complementary services.”⁴ The many types of access to networks, including retail, wholesale, interconnection, platform, and unbundled access, generally require contracts between firms.⁵

Firms also share knowledge through the formation of innovation networks.⁶ The modular organization of production means that many firms are involved in the production of components and assembly of the final product.⁷ Innovative products that contain new types of components and introduce inventions require knowledge of the technology of each component and knowledge about how to combine these technologies.⁸ Complex innovations in particular require the combination of many new technologies.⁹ Firms must make contractual agreements to obtain the components and to make sure they interoperate effectively. Firms creating complex innovations thus require contracts to coordinate inventive and innovative activities.

This Article introduces the concepts of “Intellectual Contract” (IC) and “Intellectual Tort” (IT) to advance and broaden the legal analysis of technological change and intangible assets. IC, IT, and Intellectual Property (IP) are becoming increasingly important given the rate and direction of technological change and greater focus on intangible assets. The principles of common law still apply to intangible assets.¹⁰ However,

4. DANIEL F. SPULBER AND CHRISTOPHER S. YOO, NETWORKS IN TELECOMMUNICATIONS: ECONOMICS AND LAW 39 (2009).

5. Daniel F. Spulber & Christopher S. Yoo, *Network Regulation: The Many Faces of Access*, 1 J. COMP. L. & ECON. 635 (2005).

6. See, e.g., Charles Dhanasai & Arvind Parkhe, *Orchestrating Innovation Networks* 31 ACAD. MGMT. REV. 659, 659 (2006); see generally Eric Von Hippel, *Horizontal Innovation Networks—By and for Users*, 16 INDUS. & CORP. CHANGE 293 (2007).

7. Kim B. Clark, *The Interaction of Design Hierarchies and Market Concepts in Technological Evolution*, 14 RES. POL’Y 235, 235 (1985); Rebecca M. Henderson & Kim B. Clark, *Architecture Innovation: The Reconfiguration of Existing Product Technologies and the Failure of Established Firms*, 35 ADMIN. SCI. Q. 9, 11 (1990); Karl Ulrich, *The Role of Product Architecture in the Manufacturing Firm*, 24 RES. POL’Y 419, 419 (1995).

8. Henderson & Clark, *supra* note 7, at 2.

9. Daniel F. Spulber, *Licensing Standard Essential Patents: Bargaining and Incentives to Invent* (Feb. 20, 2019) available at SSRN: <https://ssrn.com/abstract=3338997>.

10. See Richard Epstein, *Intellectual Property and the Law of Contract: The Case Against “Efficient Breach,”* 9 EUR. REV. OF CONT. L. 345 (2013); see also RICHARD EPSTEIN, *SIMPLE RULES FOR A COMPLEX WORLD* (1995).

IC, IT, and IP lack a framework that addresses the important additional implications of technological change and intangible assets.

Accordingly, this Article introduces a framework, referred to as “Intellectual Law,” to reflect major developments in legal practice and economic activity. Intellectual Law is central to myriad legal cases, including over 5,000 patent case filings per year in the U.S.¹¹ Copyright infringement cases in Federal District Court numbered 5,042 in 2015 and 3,944 in 2016.¹² Trademark infringement cases totaled 38,486 between 2009 and 2017, with 8,502 of those cases overlapping with commercial claims.¹³ Litigation in federal courts involving trade secrets has also increased.¹⁴ All areas of IP are expanding rapidly; the US Patent and Trademark Office (USPTO) has granted over 10 million patents and handled over 9 million trademark applications or registrations.¹⁵ One estimate puts the value of IP in the US at over \$5 trillion.¹⁶

This Article argues there is a need for a general Intellectual Law framework that approaches IC, IT, and IP consistently and sheds light on their interactions. The proposed new framework of Intellectual Law will contribute to Science and Technology Law.¹⁷ The purpose of the

11. Chris Barry et al., *2017 Patent Litigation Study: Change on the Horizon?*, PWC <https://www.pwc.com/us/en/forensic-services/publications/assets/2017-patent-litigation-study.pdf> (last visited Aug. 7, 2017). There is also significant trademark litigation. William Bryner, *U.S. Trademark and Unfair Competition Litigation*, INT’L TRADEMARK ASS’N (Sept. 2017), <https://www.inta.org/trademarkadministration/Documents/2017/Bryner%20-%20U.S.%20Trademark%20and%20Unfair%20Competition%20Litigation%2009142017/Bryner%20-%20U.S.%20Trademark%20and%20Unfair%20Competition%20Litigation%2009142017.pdf>.

12. *Copyright Infringement Litigation Fell 22 Percent in FY 2016*, TRACREPORTS (Nov. 21, 2016), <http://trac.syr.edu/tracreports/civil/445/>.

13. Steve Brachman, *Lex Machina’s 2017 Trademark Litigation Report Shows High Percentage of Overall Damages Awarded on Default Judgment*, IPWATCHDOG (Dec. 5, 2017), <http://www.ipwatchdog.com/2017/12/05/2017-trademark-litigation-report-damages-awarded-default-judgment/id=90683/>.

14. David Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 293 (2009).

15. See *Patents Through History*, USPTO, <https://10millionpatents.uspto.gov/> (last visited Nov. 11, 2018); *Trademark Case Files Dataset*, USPTO, <https://www.uspto.gov/learning-and-resources/electronic-data-products/trademark-case-files-dataset-0> (last visited Nov. 11, 2018); see also Stuart Graham et al., *The USPTO Trademark Case Files Dataset: Descriptions, Lessons, and Insights*, 22 J. OF ECON. & MGMT. STRATEGY 669, 669–705 (2013).

16. Robert Shapiro & Kevin Hassett, *The Economic Value of Intellectual Property*, SONECON 2, <http://www.sonecon.com/docs/studies/IntellectualPropertyReport-October2005.pdf> (last visited Nov. 11, 2018).

17. See generally CARA MORRIS & JOSEPH CARVALKO, *THE SCIENCE AND TECHNOLOGY GUIDEBOOK FOR LAWYERS* (2014); ABA Groups: *Section of Science and Technology Law*, AM. B. ASS’N, https://www.americanbar.org/groups/science_technology/about_us.html (last visited Sept. 19, 2018) (“The mission of the ABA Section of Science & Technology Law is to provide leadership on emerging issues at the intersection of law, science, and technology; to promote

framework is to approach scientific issues and technological change in a more integrated fashion. Practitioners and scholars should avoid the costs and effort of reinventing the wheel when encountering each new technological development.

IP differs from traditional property because of differences between intangible and tangible assets. These differences affect the completeness, excludability, and transferability of intangible assets. ICs differ fundamentally from traditional contracts because ICs must handle problems that arise in inducing cooperative investment in intangible assets. ITs differ from traditional torts because of the additional difficulties in determining validity and infringement of IP and finding remedies for infringement.¹⁸

Intellectual Law has become essential because technological change has increased the economic importance of intangible assets relative to that of tangible assets. Investment in knowledge is a major driver of economic growth.¹⁹ The U.S. national income accounts began to recognize R&D investment as part of Gross Domestic Product (GDP) as of 2013.²⁰ Private industry invests about two-thirds of annual R&D expenditures in the U.S., which amounted to over \$527 billion in 2017.²¹ U.S. investment in intangible assets exceeds \$1 trillion per year, with a capitalized value of over \$6 trillion.²² Intangible assets constitute about 85% of the total market value of the S&P 500 companies.²³

This Article devises the concept of Intellectual Contract to characterize an agreement to create, develop, share, or apply intangible assets involved in technological change. An IC has the standard contract features of offer, acceptance, and consideration, but differs from contracts that involve tangible assets. ICs include agreements related to traditional

sound policy and public understanding on such issues; and to enhance the professional development of its members.”).

18. For further discussion of problems related to infringement damages, see Daniel F. Spulber, *Finding Reasonable Royalty Damages: A Contract Approach to Patent Infringement*, 2019 ILL. L. REV. (forthcoming 2019).

19. Charles Hulten, *Stimulating Economic Growth Through Knowledge-Based Investment* (OECD Sci., Tech. & Industry, Working Paper No. 2, 2013), http://www.observatorioabaco.es/biblioteca/docs/412_OECD_WP_02_2013.pdf.

20. FRANCISCO MORIS ET AL., NAT’L SCI. FOUND., R&D RECOGNIZED AS INVESTMENT IN U.S. GDP STATISTICS: GDP INCREASE SLIGHTLY LOWERS R&D-TO-GDP RATIO (2015), <https://www.nsf.gov/statistics/2015/nsf15315/>.

21. U.S. R&D: *Slow Growth and Opportunities*, 2017 GLOBAL R&D FUNDING FORECAST, Winter 2017, at 7.

22. Leonard I. Nakamura, *What Is the U.S. Gross Investment in Intangibles? (At Least) One Trillion Dollars a Year!* 5 (Fed. Res. Bank of Phila., Working Paper No. 01-15, 2001).

23. Cate M. Elsten & Nick Hill, *Intangible Asset Market Value Study?*, 52 J. OF THE LICENSING EXEC. SOC’Y INT’L 245, 245–47 (2017); BARUCH LEV, INTANGIBLES: MANAGEMENT, MEASUREMENT, AND REPORTING (2001); Baruch Lev, *Remarks on the Measurement, Valuation, and Reporting of Intangible Assets* 17 (N.Y.U. Working Paper No. 2451–27468, 2003).

types of IP, that is, trade secrets, patents, trademarks, and copyrights. However, ICs also include non-traditional intangible assets such as knowledge, discoveries, inventions, innovations, and adoption of innovations that are not covered by standard IP. ICs not only include the upper tail of inventions covered by IP and IT but step in to cover the lower tail of ideas not covered by IP. ICs make adjustments to contracts to address the particular problem of creating and using knowledge. Technological change favoring intangible assets and interoperability makes ICs highly valuable and perhaps more commonly used than traditional contracts. The many types of IC identified here play an increasingly important role in fostering technological advances.

IC rules help resolve the debate over whether IP or IT is best for protecting the interests of inventors. Technological change requires cooperative investments in invention, innovation, and adoption. ICs protect the expectation interests of parties engaged in technological change: employer and employee, firm and subcontractor, and licensor and licensee. ICs not only protect inventors who make discoveries, but also innovators who apply those discoveries and adopters who demand innovations. ICs generate gains from trade that increase joint benefits for inventors, innovators, and adopters. When there are gains from trade, the inventor's returns from entering into an IC are greater than returns from either their own use of IP or an assignment to others. Because of gains from trade, ICs increase the benefits of inventors beyond what can be achieved with only IP and IT. Legal protections for inventors, innovators, and adopters thus cannot be based solely on a combination of IT and IP. Greater emphasis on IC rules by the courts within the Intellectual Law framework proposed here would address problems with both IT and IP.

I also devise the new term Intellectual Tort to designate liability rules governing the taking or infringement of intangible assets. IT includes misappropriation of trade secrets, and infringement of patents, trademarks, and copyrights. I argue that IC rules help disentangle IT rules from IP rules and overcome the shortcomings of IT rules. Many practitioners and scholars emphasize liability protections against infringement.²⁴ Daniel Crane introduces the term "Intellectual Liability" to identify the shift toward liability protections: "Instead of speaking about 'intellectual property,' it may be more appropriate to speak about

24. See, e.g., Ted Sichelman, *Purging Patent Law of "Private Law" Remedies*, 92 TEX. L. REV. 517, 519 (2013) ("[P]atent remedies mirror traditional tort law remedies by attempting to restore the patentee to the *status quo ante*—namely, the state of the world in which there is no infringement of the patent.").

‘intellectual rights’ consisting in part of intellectual property rights and in part of intellectual liability rights.”²⁵

Damage remedies based on IT, however, can fail to fully compensate IP owners or to deter infringement. In contrast, IC rules support agreements between IP owners and users that can both prevent infringement and resolve infringement disputes without the need for courts to determine compensation. When infringement does occur, the courts can use IC rules as a framework for calculating reasonable royalty damages, as I argue elsewhere.²⁶ Thus, IC rules complement IT rules by helping deter infringement and determine reasonable royalties that are compensatory.

Technological change is altering the nature of contract. ICs provide agreements needed to achieve technological change, both within the firm and among firms. I suggest that ICs have five important features that distinguish them from standard contracts involving tangible assets.

First, ICs address the lack of completeness in ownership of intangible assets. An important strength of ICs is that they help protect the vast set of property interests that standard IP does not cover. The four main categories of IP—trade secrets, patents, trademarks, and copyrights—do not fully cover commercial, scientific, and technological creations. IP is subject to challenges of validity and imperfect enforcement against infringement.²⁷ Additionally, IP typically has significant registration requirements in comparison to tangible property.²⁸ USPTO patent and trademark applications must satisfy various regulatory criteria, which entail substantial legal costs in addition to the filing fees.²⁹ The U.S. Copyright Office registers copyrights subject to various restrictions on types of works of authorship and subject matter.³⁰

25. See Daniel A. Crane, *Intellectual Liability*, 88 TEX. L. REV. 253, 254 (2009) (“Innovation incentives, once protected by property rights, are increasingly being protected by liability rights.”).

26. See Spulber, *supra* note 18.

27. John C. Paul et al., *Courts May Enforce Covenants Not to Challenge the Validity of Licensed Patents Contained in a License Agreement Settling Litigation When the Parties Clearly Waived Future Challenges to Validity*, FINNEGAN (Oct. 23, 2012), <https://www.finnegan.com/en/insights/courts-may-enforce-covenants-not-to-challenge-the-validity-of.html>.

28. F. Scott Kieff, *The Case for Registering Patents and the Law and Economics of Present Patent-Obtaining Rules*, 45 B.C. L. REV. 55, 123 (2003) (“The case for an alternative model registration system also is helpful in showing why increased scrutiny of patent applications would worsen, not improve, the present system’s performance.”).

29. Gene Quinn, *The Cost of Obtaining a Patent in the U.S.*, IPWATCHDOG (Apr. 4, 2015), <http://www.ipwatchdog.com/2015/04/04/the-cost-of-obtaining-a-patent-in-the-us/id=56485/>; see Rebecca Tushnet, *Registering Disagreement: Registration in Modern American Trademark Law*, 130 HARV. L. REV. 867 (2017).

30. See 17 U.S.C. § 102 (2018).

Second, ICs remedy problems of exclusion of access to intangible assets because ICs help determine how parties will share the returns and control over intangible assets. Without contracts, it can be difficult to protect intangible assets. The law treats tangible and intangible property differently because IP limits exclusivity, transferability, and duration of ownership.³¹ Various court cases, statutes, and administrative decisions have weakened legal protections for IP. Although the Patent Act gives patents “the attributes of personal property,” these protections are incomplete.³² The Supreme Court ruled unanimously in *eBay Inc. v. MercExchange, L.L.C.* that “the creation of a right is distinct from the provision of remedies for violations of that right.”³³ Physical barriers provide limited protection because knowledge is readily transferable and easy to imitate or appropriate. Secrecy may not be feasible because offering IP for sale or license requires disclosing the knowledge. Using IP within an organization and with business partners also requires continual sharing of knowledge.

Third, ICs handle non-rivalrous usage of intangible assets, a problem that generally does not arise with tangible assets. Intangible assets can provide services to multiple users at once.³⁴ ICs such as license and cross-license agreements provide access to intangible assets for multiple users and handle in-kind exchanges of access to intangible assets. ICs can bundle intangible assets such as licenses for patent portfolios, as well as bundle intangible assets with tangible assets, goods, and services. ICs also can unbundle intangible assets by specifying conditions of use through the grant of rights.

Fourth, ICs address problems in designing incentives for what I refer to here as “exploratory performance.” An IC must monitor and reward the agent’s performance in exploring uncharted waters. By its very nature, technological change is a leap into the unknown. Economic analysis identifies agency costs that arise from difficulties in observing an agent’s hidden actions or hidden information.³⁵ Contracts must be based on performance because outputs are observable and verifiable while inputs are not. The design of an IC, however, encounters difficulties in determining performance targets and observing performance. It is hard

31. Peter S. Menell, *The Property Rights Movement’s Embrace of Intellectual Property: True Love or Doomed Relationship*, 34 *ECOLOGY L. Q.* 713, 747 (2007); Peter S. Menell, *Intellectual Property and the Property Rights Movement*, 30 *REG.* 36, 39 (2007).

32. See 35 U.S.C. § 261 (2018).

33. *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 392 (2006).

34. There is non-rivalrous usage of some types of tangible assets if demand is constrained below the capacity of the asset. For example, there is non-rivalrous usage of a bridge or a park if demand is less than capacity and there are no congestion externalities. See Chizoba Mora, *How Is Computer Software Classified as an Asset?*, *INVESTOPEDIA* (May 15, 2018, 11:50 AM), <https://www.investopedia.com/ask/answers/09/computer-software-intangible-asset.asp>.

35. Epstein, *supra* note 10, at 6.

to know what the outcomes of invention, innovation, and technology adoption will be. This presents a greater challenge than traditional agency costs. This also makes it difficult to determine the intent of the parties as well as to find remedies for breach of contract. ICs provide incentives for exploration by rewarding measures of performance that are observable and verifiable rather than inventive effort.

Fifth, ICs provide mechanisms for addressing fundamental uncertainty associated with invention, innovation, and adoption. Technological change involves particular types of statistical, discovery, creativity, and market uncertainty. This uncertainty distinguishes ICs from standard contracts involving routine activities and risky investments in tangible assets. Fundamental uncertainty generates benefits from contingent contracting.³⁶ An IC must address the well-known trade-off between the benefits and costs of contingent contracts.³⁷ Contract law and the costs of contracting provide incentives for simple contract forms.³⁸ ICs offer basic mechanisms such as royalties and options that address the uncertainties of technological change.³⁹

I identify five main types of ICs: employment, outsourcing, joint venture and consortium, license, and platform. Firms enter into employment contracts with scientific and technical personnel who conduct invention and innovation within the firm. Firms use outsourcing contracts with specialist firms and supply chain management companies that develop inventions and innovations. Firms form joint venture and consortium contracts to establish research joint ventures (RJVs) and R&D consortia. Joint venture and consortium contracts allow firms to share the costs, risks, and outputs of invention and innovation. Firms create license contracts for usage of patents, trademarks, copyrights, and business knowledge. Finally, firms apply platform contracts that bring together providers and adopters of technology. Firms enter into platform contracts with for-profit intermediaries and with cooperative institutions such as patent pools and other Collective Rights Organizations (CROs).⁴⁰

36. *Id.* at 10.

37. *Id.* at 8.

38. Alan Schwartz & Joel Watson, *The Law and Economics of Costly Contracting* 2–31 (John M. Olin Center for Stud. In L., Econ., & Pub. Pol’y, Working Paper No. 264, 2001) (“Contract law encourages courts to search thoroughly for the parties’ actual intentions in creating the contract and in renegotiating it. We show that this search has yielded mandatory legal rules that make it extremely difficult for parties to restrict renegotiation, and that can increase greatly the cost of creating sophisticated contracts. As a consequence, parties now have legal incentives to use the more simple contract forms . . .”).

39. Joaquin Poblete & Daniel Spulber, *Managing Innovation: Optimal Incentive Contracts for Delegated R&D with Double Moral Hazard*, 95 EUR. ECON. REV. 38 (June 2017).

40. Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CAL. L. REV. 1293, 1358 (1996).

I. INTELLECTUAL LAW

Developing the Intellectual Law framework requires a coherent treatment of invention, innovation, and technology adoption. However, legal protections for intangible assets are a mixture of property and tort. Applications of property and tort to intangible assets fail to address consent in a consistent way. As a consequence, these protections fail to perform effectively both property and tort functions. Recognizing the widespread use of various forms of ICs would help bring consistency to Intellectual Law because it addresses the key question of consent for agreements involving intangible assets. Courts can apply ICs to improve legal protections for the creation and application of intangible assets.

A. *The Conflict Between IT and IP*

Guido Calabresi and Douglas Melamed distinguish between property and tort in terms of who has consent.⁴¹ Protections are based on property if the owner's consent to sell is necessary for transfers.⁴² Protections are based on tort if the taker's consent to buy is sufficient for transfers.⁴³ This is because someone taking the asset determines whether they want to pay compensation by choosing to infringe. The liability rule effectively removes the owner's consent to sell, whether or not the taking is intentional.⁴⁴ The distinction between property and tort rules provides clarity for tangible assets that may be absent for intangible assets.

Legal protections for intangible assets—currently based on a haphazard combination of IT and IP—are incomplete because they do not address consent in a consistent way. Protections for intangible assets are based partly on IT because damage remedies remove the IP owner's consent to sell an intangible asset. Damage remedies make the infringer's consent to buy sufficient for ongoing transfers. Based on this perspective, some have characterized patent infringement as a “strict liability” tort.⁴⁵

41. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972) (“An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller. . . . Whenever someone may destroy the initial entitlement if he is willing to pay an objectively determined value for it, an entitlement is protected by a liability rule. This value may be what it is thought the original holder of the entitlement would have sold it for.”).

42. *Id.*

43. *Id.*

44. Richard A. Epstein, *The Clear View of the Cathedral: The Dominance of Property Rules*, 106 YALE L.J. 2091, 2091 (1997) (“[A] liability rule denies the holder of the asset the power to exclude others or, indeed, to keep the asset for himself.”).

45. Mark A. Lemley, *Should Patent Infringement Require Proof of Copying?*, 105 MICH. L. REV. 1525, 1525 (2006) (“Patent infringement is a strict liability offense.”); Roger Blair &

Following this approach to patent infringement, various limitations on strict liability would further reduce protections for inventions.⁴⁶ Protections for intangible assets are based partly on IP because the IP owner has some rights to exclude and so must consent to license or sell an intangible asset.⁴⁷ However, IP rights often limit exclusivity, again removing the IP owner's consent to sell.⁴⁸

The Supreme Court's unanimous *eBay* decision illustrates the mixture of property and tort approaches.⁴⁹ Problems arise because the Court did not address *consent* in a consistent way. The *eBay* decision has created some confusion by conflating IT and IP.⁵⁰ The Court in *eBay* weakens IP in comparison to tangible property by reducing the consent of the IP owner as seller.⁵¹ The infringer's consent as buyer can dominate the IP owner's consent as seller, converting property remedies to tort remedies.

The *eBay* decision limits injunctions for intangible assets by applying the four-factor test for issuing injunctions to patent infringement.⁵² The first factor, irreparable harm, is a particularly high hurdle for the IP owner. Second, requiring the IP owner to show that remedies are inadequate compensation is an additional burden that replaces IP with IT rules. Third, consideration of the balance of hardships between plaintiff and defendant differs substantially from property rights in tangible assets. Consideration of the balance of hardships combines the IP owner's consent as seller with the infringer's consent as buyer. Finally, the public interest criterion places IP rights in a different category from tangible property.

Thomas F. Cotter, *Strict Liability and Its Alternatives in Patent Law*, 17 BERKELEY TECH. L.J. 799, 800 (2002) [hereinafter Blair & Cotter, *Strict Liability*] ("Patent infringement is a strict liability tort in the sense that a defendant may be liable without having had any notice, prior to the filing of an infringement action, that her conduct was infringing."); Roger Blair & Thomas F. Cotter, *An Economic Analysis of Damages Rules in Intellectual Property Law*, 39 WM. & MARY L. REV. 1585 (1998).

46. Blair & Cotter, *Strict Liability*, *supra* note 45, at 806 (suggesting that liability need not be considered strict because in some cases giving notice is required for liability).

47. *Id.*

48. *Id.*

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

50. *See id.*

51. *See id.*

52. *See id.* at 388, 393 ("The traditional four-factor test applied by courts of equity when considering whether to award permanent injunctive relief to a prevailing plaintiff applies to disputes arising under the Patent Act. That test requires a plaintiff to demonstrate: (1) that it has suffered an irreparable injury; (2) that remedies available at law are inadequate to compensate for that injury; (3) that considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction. . . . [A] permanent injunction will issue once infringement and validity have been adjudged.").

Andrew Beckerman-Rodau observes that *eBay* is “part of a broad attack on the current U.S. patent system.”⁵³ David McGowan argues that the Court in *eBay* “reversed the longstanding presumption in favor of permanent injunctive relief for proven patent infringement.”⁵⁴ Evidence suggests that post-*eBay* district courts continue to grant permanent injunctions.⁵⁵ Injunctions are more likely when the IP owner competes with the infringer.⁵⁶

Richard Epstein argues against exclusively using damages for infringement of IP in the absence of the possibility of injunctive relief.⁵⁷ Infringement would then function as a viable option for the infringer, potentially leading to excessive infringement.⁵⁸ Epstein compares damages for infringement to the general problem of damages for breach of contract.⁵⁹ He criticizes the “efficient breach” approach when expectation damages are the only remedy for breach of contract.⁶⁰ Without the possibility of injunctive relief, expectation damages function as an option for the party contemplating breach, which may reduce incentives to contract.⁶¹

The courts’ standard approach to resolving patent infringement disputes further illustrates the mixture of property and tort. Courts typically apply the “hypothetical negotiation” approach to calculating reasonable royalty damages.⁶² The hypothetical negotiation approach combines property and tort because it tries to imagine both what a willing licensor would accept and what a willing licensee would accept.⁶³ The

53. Andrew Beckerman-Rodau, *The Supreme Court Engages in Judicial Activism in Interpreting the Patent Law in eBay, Inc. v. MercExchange, L.L.C.*, 10 TUL. J. TECH. & INTELL. PROP. 165, 165 (2007).

54. David McGowan, *Irreparable Harm*, 14 LEWIS & CLARK L. REV. 577, 579 (2010).

55. See Rachel M. Janutis, *The Supreme Court’s Unremarkable Decision in eBay Inc. v. MercExchange, L.L.C.*, 14 LEWIS & CLARK L. REV. 597, 601, 604 (2010); Benjamin Peterson, *Injunctive Relief in the Post-eBay World*, 23 BERKELEY TECH. L. J. 193, 196 (2008); Douglas Ellis et al., *The Economic Implications (and Uncertainties) of Obtaining Permanent Injunctive Relief After eBay v. MercExchange*, 17 FED. CIR. B. J. 437, 441 (2008).

56. Janutis, *supra* note 55, at 605.

57. Epstein, *supra* note 10, at 5.

58. *Id.* at 24.

59. *Id.* at 6–8.

59. *Id.*

61. *Id.* at 24–25.

62. John C. Jarosz & Michael J. Chapman, *The Hypothetical Negotiation and Reasonable Royalty Damages: The Tail Wagging the Dog*, 16 STAN. TECH. L. REV. 769, 772 (2013) (“[T]he hypothetical negotiation construct was originally introduced simply as one of many considerations to estimate such damages. It has since evolved into the primary tool used to determine reasonable royalty damages.”).

63. *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, 318 F. Supp. 1116, 1121 (S.D.N.Y. 1970) (“The [willing buyer and willing seller] rule is more a statement of approach than a tool of analysis. It requires consideration not only of the amount that a willing licensee would have paid for the patent license but also of the amount that a willing licensor would have accepted.”).

acceptance of the willing licensor is the property side of the law and the acceptance of the willing licensee is the tort side of the law. So, the hypothetical negotiation tries to simultaneously satisfy property and tort remedies.

The hypothetical negotiation, however, may fail to satisfy both property and tort remedies. One reason for this is that the hypothetical benefit to the infringer may be less than the hypothetical harm to the patent holder. If the infringer's benefit from adopting the technology is less than the patent holder's cost of providing the technology, there is no basis for an economically efficient transaction. The transaction would yield negative net benefits.

If the infringer's benefit from adopting the technology is less than the cost to the patent holder of providing the technology, there is no royalty that would support an exchange. The patent holder would not give consent as seller for any royalty that does not cover the cost of providing the technology because the royalty would not be compensatory. So, the hypothetical negotiation would not protect property interests.

Conversely, the infringer would not consent as buyer to any royalty that would be greater than the benefits of implementing the technology. The patent holder thus would not be compensated for the damages from infringement. So, the hypothetical negotiation would not satisfy tort requirements.

Further, the hypothetical negotiation also fails to provide either property or tort remedies because it undertakes the impossible task of determining the property owner's expectations and the infringer's expectations before infringement occurs.⁶⁴ This requires knowledge not available to either the patent holder or the infringer, let alone the court. The passage of time and the resolution of uncertainty will change the infringer's benefit from infringement and the patent holder's damages from infringement. Damages based on the hypothetical negotiation are unlikely to reflect either the patent holder's cost as seller or the infringer's benefit as buyer.

The courts apply two damages calculations that are subject to similar problems.⁶⁵ First, the "bottom-up" approach calculates reasonable royalty damages as a share of the infringer's benefit based on the incremental value of the patents to the infringer.⁶⁶ This approach requires not only determining the infringer's direct valuation of the patented technology,

64. *Id.*

65. *Id.*

66. Gregory K. Leonard & Mario A. Lopez, *Determining RAND Royalty Rates for Standard-Essential Patents*, 29 ANTITRUST 86, 88 (2014) ("The bottom-up approach is consistent with the conceptual definition of RAND and is commonly performed in patent infringement cases.").

but also the valuation of the best alternative.⁶⁷ Second, the “top-down” approach is based on marking down the infringer’s profit and apportioning that profit among multiple technologies.⁶⁸ The top-down approach appears in *In re Innovatio* and *TCL Communications v. Ericsson*.⁶⁹

Both of these damage calculations are based on the infringer’s benefits.⁷⁰ The two methods represent tort solutions to patent infringement because they are sufficient to insure the infringer’s consent as buyer for ongoing infringement. These methods may not necessarily be compensatory, however, because the awarded damages may be less than the patent holder’s costs—even if the patent holder’s costs are less than the infringer’s benefits. These methods are a shift from IP to IT because they tend to remove the owner’s consent as seller.

B. Untangling IT and IP

IC rules provide guidance in untangling IT and IP. Private agreements should be more efficient than outcomes created by courts because the parties know more about their situation than do the courts. Transaction costs can reduce the efficiency of private agreements, but such costs tend to be lower than litigation costs.

The courts can untangle IT from IP by separating compensation from injunction. An IC protects the expectations of the parties to the agreement. If an IC is breached, it is necessary to compensate the injured party for harm caused by the breach. The courts should at least provide compensation to owners of IP for infringement that has already occurred. The damages to IP owners should include all of the economic costs due to the infringement, including transaction costs. The damages also can be tripled if the infringer engaged in “egregious infringement behavior.”⁷¹

67. *Id.*

68. *Id.* at 89.

69. *In re Innovatio IP Ventures, LLC Patent Litigation*, No. 11-C-9308, 2013 WL 5593609 (N.D. Ill. Oct. 3, 2012); *TCL Commc’ns Tech. Holdings, Ltd. v. Telefonaktenbologet LM Ericsson*, No. SACV 14-00341 JVS (ANx), 2016 WL 4150033 (C.D. Cal. July 25, 2016); see Jason Rantanen, *TCL v. Ericsson: The First Major U.S. Top-Down FRAND Royalty Decision*, PATENTLYO (Dec. 27, 2017), <https://patentlyo.com/patent/2017/12/contreras-ericsson-decision.html>; Richard Vary, *Supersize This: Unwired Planet American Style*, BIRD & BIRD (Dec. 2017), <https://www.twobirds.com/en/news/articles/2017/global/supersize-this-unwired-planet-american-style>.

70. Leonard & Lopez, *supra* note 66, at 86–87.

71. See *Halo Elecs. Inc. v. Pulse Elecs. Inc.*, 136 S. Ct. 1923, 1925 (2016); *Stryker Corp. v. Zimmer, Inc.*, 782 F.3d 649, 661 (Fed. Cir. 2015); George W. Jordan III, *Halo v. Pulse: A New Chapter for Willfulness and Enhanced Patent Damages*, LANDSLIDE (Mar.–Apr. 2017), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2016-17/march-april/halo_v_pulse_new_chapter_willfulness_and_enhanced_patent_damages/.

The courts should not necessarily rely on compensation for infringement that has not yet occurred. Forward-looking damages give the infringer consent as the buyer and remove the owner's consent as the seller. This approach weakens IP and leads to an inefficient appropriation of technology. Instead, courts should impose an injunction when necessary to prevent future infringement.⁷² This restores the consent of the owner of the intangible asset.

An injunction not only mitigates future harm but provides incentives for the parties to negotiate an IC. If the benefit to the infringer is greater than the cost to the owner, the parties benefit from an IC; an injunction should thus lead to an IC. If the benefit to the infringer is less than the cost to the owner, then the parties will not benefit from an IC, but an injunction will stop the infringement. Injunctions protect the IP rights of the owners of the intangible assets by restoring their consent as seller.

Infringement is technology transfer in the absence of an IC. Infringement represents a failure to contract, whether or not infringement is intentional.⁷³ Failure to reach a contractual agreement combined with continued usage of the intangible asset is likely to lead to an infringement dispute. An IC prevents the infringement dispute and can also resolve an infringement dispute after it has already begun.

IC rules also help calculate damage remedies for infringement. Rather than imagining the situation of the parties before infringement began, it is necessary to determine the actual harm from infringement. As I discuss in detail elsewhere, the court in a patent case gathers evidence that fills in many of the terms of a patent license agreement.⁷⁴ The evidence includes the identity of the parties, their business relationship, and the nature of the IP being transferred. The evidence indicates the extent of the infringement and helps determine the harm to the owner of the intangible assets.

In infringement disputes, courts should construct what I have referred to elsewhere as an "informed contract."⁷⁵ This approach is consistent with IC rules and replaces the flawed hypothetical negotiation. The informed contract builds on the information revealed by the patent case to estimate the harm to the patent holder. The patent holder's lost profits and reasonable damages should be based on infringement that actually occurred. Courts should not attempt the impossible task of constructing imagined expectations for a negotiation that did not occur.

72. 35 U.S.C. § 283 (2018) ("The several courts having jurisdiction of cases under this title may grant injunctions in accordance with the principles of equity to prevent the violation of any right secured by patent, on such terms as the court deems reasonable.").

73. Spulber, *supra* note 18, at 21.

74. Spulber, *supra* note 18, at 7.

75. Spulber, *supra* note 18, at 3.

In determining damages for infringement, the IC approach suggests that courts should use royalties from comparable ICs. These royalties from comparable license contracts should be adjusted based on information revealed by the patent case. In particular, royalties should reflect the increase in market value of a license that comes with a patent found to be valid and infringed upon. Royalties for Standard Essential Patents (SEPs) should reflect the added market value of the patent license that is revealed by inclusion of the patent in technology standards chosen by a Standard Setting Organization (SSO). Other characteristics of patents can raise or lower the market value of licenses and can be used to adjust royalties from comparable licenses.

If there are no comparable patent licenses, reasonable royalty damages can be estimated by using the market prices of patents. I have spelled out the “market value method” of calculating reasonable royalty damages.⁷⁶ The market prices of patents provide information about expected returns from own use and total royalties from multiple licensing agreements. These can be apportioned among infringers to determine the royalties that would have been received but for the infringement.

IT, or liability for infringement, does not offer sufficient legal support for technological change. IT does little to deter infringement of ideas and provides no guidelines for cooperative agreements. Technological change cannot depend only on compensating patent holders for infringement. Although recovery of lost profits or reasonable royalty damages may serve as remedies for infringement, this is not sufficient to induce cooperative investment in creating and applying new ideas. IP protections are necessary to preserve incentives to form ICs, thus protecting expectation interests.

C. ICs and the “Market for Innovative Control”

IC rules help resolve the ongoing debate over whether IP or IT provides the best protections for inventors. The protection of the interests of inventors depends on the combination of property, tort, and contract rules. ICs generate gains from trade for all parties, thus enhancing the benefits for inventors beyond what IP and IT protections can provide. ICs complement IP and IT protections by supporting commercialization and cooperative investment.

ICs are the main transaction method for what I have termed the “market for innovative control.”⁷⁷ ICs allocate both returns from intangible assets and rights of control over innovation using those assets.

76. Spulber, *supra* note 18, at 7 (describing the “market value method” of calculating reasonably royalty damages).

77. Daniel F. Spulber, *How Patents Provide the Foundation of the Market for Inventions*, 11 J. COMPETITION L. & ECON. 271, 274 (2015).

ICs protect the continual stream of discoveries and extensive sharing of knowledge required for cooperative investment. ICs involve investment in disembodied technology as well as technology embodied in goods and services. The characteristics of technological change suggest increased usage of ICs in comparison to standard contracts. Investment continues to shift away from tangible assets and toward intangible assets. Virtual inventions and innovations represent a shift away from hardware innovations and toward software innovations.⁷⁸ For example, improvements in products, production processes, and business methods may take the form of software upgrades rather than new equipment with improved capabilities. Such innovation will take the form of intangible assets. Technology transfers and upgrades will require ICs that protect expectation interests and IP.

Technological change that increases connectivity and knowledge sharing may require new types of contract provisions. Innovations in IoT involve a significant increase in connectivity among firms as well as between firms and customers. The International Telecommunications Union (ITU) defines the IoT as: “A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”⁷⁹ According to the ITU, “The IoT is expected to greatly integrate leading technologies, such as technologies related to advanced machine-to-machine communication, autonomic networking, data mining and decision-making, security and privacy protection, and cloud computing, with technologies for advanced sensing and actuation.”⁸⁰ The ITU identifies various types of business roles in IoT, including providers of platforms, networks, devices, and applications.⁸¹ These business roles are likely to require ICs.

Advances in AI also suggest greater use of ICs. Employees and managers working with AI will jointly generate knowledge and inventions. It will be necessary to specify how to monitor and reward the performance of employees and managers who interact with AI systems. It will also be necessary to determine inventions and innovations created by employees that work with AI systems. Related considerations apply to contractual relationships between firms that involve AI systems. It may be necessary to specify performance in terms of both the activities of individuals and AI systems.

78. MÉNIÈRE ET AL., *supra* note 1, at 20.

79. INT’L TELECOMM. UNION, SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS (June 2012), https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items.

80. *Id.* at 2.

81. *Id.* at 4.

The market for innovative control depends on the broad framework of Intellectual Law. Protections for IP rights and other aspects of IP improve the efficiency of transactions in the market for innovative control.⁸² Extending and enhancing these traditional protections, ICs allocate residual returns and residual control rights from IP and support cooperative investment in invention, innovation, and adoption. ICs are important for innovation by established firms and entrepreneurs because they protect the expectation interests of inventors, innovators, and adopters. ICs thus support cooperative agreements to develop and apply technology. These agreements increase the benefits of inventors beyond what they could obtain through own use and transfers of inventions. So, ICs promote the interests of inventors beyond what property or liability rules alone could achieve.

Efficient economic activity depends on a combination of contractual agreements and property rights. Contractual agreements require well-defined property rights for tangible assets that provide completeness, exclusivity, and transferability. In turn, owners of tangible property, including land, structures, inventory, and capital equipment, cannot realize the full economic value of those assets simply from own use and transfer of assets to others. Property owners need contracts that support cooperation over time and investment in tangible assets. A market system requires contracts for employment, production, construction, procurement, distribution, and finance.

Technological change also depends on a combination of contractual agreements and property rights. IP provides the foundation of the market for innovative control by improving efficiency and gains from trade from ICs. However, even a well-functioning IP system is not sufficient to protect the interests of inventors, innovators, and adopters. Owners of IP cannot rely only on own-use and transfers of IP. ICs allocate both residual returns and residual rights of control over how inventions are developed and applied to generate innovations. Through ICs such as licensing agreements, patent holders and technology adopters determine how technology will be applied. Firms require ICs to form agreements with employees, suppliers, partners, distributors, investors, and customers.

ICs differ from standard contracts because the characteristics of intangible assets differ from those of tangible assets. Firms form ICs with managers and specialized employees to carry out invention, innovation, and adoption. Firms form ICs with other firms to outsource R&D and to share inventions and innovations. The development and application of inventions and innovations require cooperative investment to create and develop intangible assets. ICs realize many benefits that are beyond the reach of own use or immediate exchange of intangible assets.

82. Spulber, *supra* note 77.

An IC involves those intangible assets associated with invention, innovation, and adoption. Not all intangible assets are related to technological change.⁸³ According to the International Accounting Standards (IAS) 38, “An intangible asset is an identifiable non-monetary asset without physical substance. Such an asset is identifiable when it is separable, or when it arises from contractual or other legal rights. Separable assets can be sold, transferred, licensed, etc.”⁸⁴ The legal rights and obligations in a contract also are intangible assets, but not all contracts are ICs.⁸⁵

The market for innovative control allocates both returns of innovation and control over innovative investment decisions. The market for technology resembles the stock market, which allocates both residual returns and residual rights of control over corporate investment decisions. The market for innovative control includes licensing and cross-licensing agreements for IP and specialized agreements to develop and apply inventions and innovations over time. The market for innovative control also includes the transfer of intangible assets and the sale of inventions and innovations that are embodied in goods and services. The market for innovative control further includes mergers and acquisitions (M&A) that transfer ownership of corporations’ intangible assets. The market for innovative control also encompasses financing of invention and innovation, including venture capital.⁸⁶

Despite its limitations, IP improves transaction efficiencies in the market for innovative control. In addition to exclusivity and transferability, IP reduces transaction costs and improves the efficiency of contracts by offering disclosure, certification, standardization, and divisibility.⁸⁷ IP provides a basis for licensing, cross-licensing, and other

83. IAS 38—*Intangible Assets*, DELOITTE, <https://www.iasplus.com/en/standards/ias/ias38> (last visited Feb. 9, 2019) (Examples of intangible assets include: “[P]atented technology, computer software, databases and trade secrets; trademarks, trade dress, newspaper mastheads, internet domains; video and audiovisual material (e.g. motion pictures, television programmes); customer lists; mortgage servicing rights; licensing, royalty and standstill agreements; import quotas; franchise agreements; customer and supplier relationships (including customer lists); marketing rights.”).

84. IAS 38 *Intangible Assets*, INT’L FIN. REPORTING STANDARDS FOUND., <https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/> (last visited Feb. 9, 2019).

85. Robert F. Reilly, *Valuation of Contract-Related Intangible Assets*, THE PRACTICAL LAWYER, Dec. 2013, at 37, 38, http://www.willamette.com/pubs/presentations3/reilly_contract_intangibles_tpl2013.pdf (“The contract document (or the oral agreement) itself is not the intangible asset. The legal rights and duties of the contract are the intangible asset.”).

86. See DANIEL F. SPULBER, *THE INNOVATIVE ENTREPRENEUR* 27–29 (2014).

87. Daniel F. Spulber, *Public Prizes Versus Market Prices: Should Contests Replace Patents?*, 97 J.PAT. & TRADEMARK OFF. SOC’Y 690 (2015).

ICs. IP supports ICs involving the joint development and allocation of inventions and innovations.

Robert Merges emphasizes the general contributions of property to contracting, and these contributions are particularly applicable to IP.⁸⁸ Merges points out that property provides “precontractual liability,” which protects the disclosure of information before a contract is formed.⁸⁹ Merges further observes that property provides “enforcement flexibility” after a contract is formed.⁹⁰ Merges emphasizes the importance of this interaction between contract and property with modular production and specialized firms.⁹¹

IP enhances coordination in contractual relationships. Scott Kieff emphasizes that patents “facilitate investment in the complex, costly, and risky commercialization activities required to turn nascent inventions into new goods and services.”⁹² Kieff observes that “This commercialization approach sees property rights in IP serving a role akin to beacons in the dark, drawing to themselves all of those potential complementary users of the IP-protected-asset to interact with the IP owner and each other.”⁹³ Kieff argues that the coordination provided by IP leads to contracts: “This helps them each explore through the bargaining process the possibility of striking contracts with each other.”⁹⁴

IP generates economic benefits by supporting market transactions rather than simply own use of intangible assets. A report by the Economics and Statistics Administration and the USPTO frames the benefits of IP in terms of economic activities:

88. Robert P. Merges, *A Transactional View of Property Rights*, 20 BERKELEY TECH. L.J. 1477 (2005).

89. *Id.* at 1488.

90. *Id.*

91. *Id.* at 1514–19.

92. F. Scott Kieff, *Property Rights and Property Rules for Commercializing Inventions*, 85 MINN. L. REV. 697, 703 (2000); see also Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265, 266 (1977); John F. Duffy, *Rethinking the Prospect Theory of Patents*, 71 U. CHI. L. REV. 439, 439 (2004); Paul J. Heald, *A Transaction Costs Theory of Patent Law*, 66 OHIO ST. L.J. 473, 508 (2005).

93. Email from the Honorable F. Scott Kieff, Comm’r, U.S. Int’l Trade Comm’n, to U.S. Fed. Trade Comm’n & Dep’t of Justice, (Sept. 23, 2016) [hereinafter Kieff, FTC & DoJ Joint IP-AT Guidelines Email], <https://www.ftc.gov/policy/public-comments/2016/09/30/comment-00006> (expressing his views on the United States Federal Trade Commission’s and the United States Department of Justice Antitrust Division’s Joint Guidelines for the Licensing of Intellectual Property); see also F. Scott Kieff & Troy A. Paredes, *The Basics Matter: At the Periphery of Intellectual Property*, 73 GEO. WASH. L. REV. 174, 179 (2004).

94. Kieff, FTC & DoJ Joint IP-AT Guidelines Email, *supra* note 93.

- Providing incentives to invent and create;
- Protecting innovators from unauthorized copying;
- Facilitating vertical specialization in technology markets;
- Creating a platform for financial investments in innovation;
- Supporting entrepreneurial liquidity through mergers, acquisitions, and IPOs;
- Supporting licensing-based technology business models; and
- Enabling a more efficient market for trading in technology and know-how.⁹⁵

Notice that each of these economic activities is based on parties forming ICs, including invention, innovation, finance, licensing, and transactions in the market for technology.

Conversely, IP owners rely on ICs for the development, commercialization, and application of intangible assets. The increasing importance of technological change in the economy has generated a burgeoning market for innovative control.⁹⁶ Owners of intangible assets not only obtain a stream of returns, but also have rights of control over inventions, innovations, and adoption. The market value of intangible assets is the present value of the stream of returns and control rights.

IC relationships provide mechanisms of commercialization for IP holders. Raymond Nimmer points out that “commercialization, which depends on contractual relationships, constitutes one of the core mechanisms by which information is developed and distributed. It is a central part of intellectual property law ‘bargain’ and should be recognized as such.”⁹⁷ Nimmer observes: “Only the most naive observer, or one with a clear political agenda, can look at the intellectual property laws and their history and suggest that policy in the property sphere trumps or precludes the influence of contract.”⁹⁸ For example, contracts

95. JUSTIN ANTONIPILLAI & MICHELLE K. LEE, USPTO, INTELLECTUAL PROPERTY AND THE U.S. ECONOMY: 2016 UPDATE 3 (last visited Mar. 28, 2018), <https://www.uspto.gov/sites/default/files/documents/IPandtheUSEconomySept2016.pdf>.

96. Spulber, *supra* note 77, at 6.

97. Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827, 888 (1998). Nimmer also states that “property rights are routinely transferred, waived, released and licensed. Contracts provide the means for the development and commercial exploitation of information assets.” *Id.* at 830.

98. *Id.* at 827.

such as online “click-wrap” agreements provide “private ordering” for information and knowledge sharing.⁹⁹

Because antitrust policy generally targets anti-competitive conduct rather than ownership rights, antitrust policy toward innovation correspondingly targets anti-competitive conduct rather than ownership of intangible assets. The Department of Justice (DOJ) Antitrust Division and the Federal Trade Commission (FTC) both recognize that IP owners depend on contracts to realize the benefits from intangible assets.¹⁰⁰ The title of the DOJ and FTC policy thus addresses a type of IC rather than IP: “Antitrust Guidelines for the Licensing of Intellectual Property.”¹⁰¹ Further, the Antitrust Guidelines acknowledge the central importance of contracts when dealing with IP: “The owner of intellectual property has to arrange for its combination with other necessary factors to realize its commercial value.”¹⁰²

ICs and IP perform different economic functions, although both have present values. An IC can be described as a joint investment project that generates a stream of returns over time and is subject to uncertainty. An immediate exchange of IP involves the transfer of a bundle of rights that generates a stream of returns over time that is subject to uncertainty. In both cases, the stream of returns over time refers to the stream of revenues minus costs at each date.

An IC provides a mechanism for cooperation over time to implement technological change. An IC spells out the performance of activities involved in technological change. Adjusting investment over time in light of new information increases the expected value of investment projects in comparison to projects that do not adjust investment levels.¹⁰³

As with contracts generally, an IC protects the expectation interests of the parties and provides incentives for investment. Because contracts are voluntary, the parties only enter into an IC if they anticipate benefits from

99. See Sharon K. Sandeen, *A Contract by Any Other Name Is Still a Contract: Examining the Effectiveness of Trade Secret Clauses to Protect Databases*, 45 IDEA 119, 122 (2005) (discussing the relationship between contracts and IP); David Friedman, *In Defense of Private Orderings: Comments on Julie Cohen's Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1151, 1152 (1998); J. H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875, 904 (1999); Robert P. Merges, *The End of Friction? Property Rights and Contract in the “Newtonian” World of On-Line Commerce*, 12 BERKELEY TECH. L.J. 115, 126 (1997).

100. FED. TRADE COMM’N, ANTITRUST GUIDELINES FOR THE LICENSING OF INTELLECTUAL PROPERTY 4 (Jan. 12, 2017), https://www.ftc.gov/system/files/documents/public_statements/1049793/ip_guidelines_2017.pdf.

101. *Id.*

102. *Id.*

103. See, e.g., AVINASH K. DIXIT & ROBERT S. PINDYCK, INVESTMENT UNDER UNCERTAINTY 2 (1994).

the bargain. To benefit from the bargain, both parties must receive gains from trade. The terms of the contract allocate gains from trade and define future performance.

The parties' expectation interests refer to the anticipation of benefits in the future. A contract protects a party's expectation interests if the party realizes the value of the contract, even if the promised performance does not occur. The legal use of the term "expectation" refers to the parties' present value of future benefits from the contract. However, this can differ from the use of the term "expectation" in the fields of probability and statistics.

The present value of a contract depends on the discount rate and expectations about uncertain outcomes. In the absence of uncertainty, the total benefits of an IC equal the present value of the stream of future returns discounted using the appropriate rate of interest. The parties to an IC will divide the present discounted value of the stream of future returns. The benefits of owning IP also equal the present discounted value of the stream of future returns obtained by using and licensing the IP. In a competitive market, the price of the IP should equal the present discounted value of the stream of future returns. When uncertainty is present, estimating the benefits of an IC and the benefits of owning IP involve expectations about the resolution of uncertainty. Combined, the discounting of future benefits and the expectation of the outcome of uncertainty generate an expected present discounted value.¹⁰⁴

An IC enhances the value of IP because cooperation generates gains from trade. The parties create additional economic value relative to own-use or an immediate exchange of intangible assets. An IC protects the expectation interests of both parties. Let V denote the present value of the discounted stream of net benefits expected by parties forming an IC. Let U denote the total opportunity costs of the parties, which equals the present value of the discounted stream of expected benefits forgone. Then, $V - U$ denotes total gains from trade for the two parties entering an IC.

Licensing agreements are a form of IC covering the usage of all types of intangible assets: patents, trademarks, copyrights, and trade secrets. Suppose that V is the net benefit of the licensee and suppose also that the IP holder derives no additional benefits from the agreement. The benefit V includes the returns to investment by the licensee in applying the technology and returns to investment in complementary assets net of the costs of investment. Suppose that the licensee has no opportunity costs

104. There are difficulties in forming expectations about future events. See discussion *infra* Section IV. Also, calculating the expected present discounted value of a stream of benefits requires adjusting either discount rates or the expected value of benefits to account for the costs of risk. See Alexander A. Robichek & Stewart C. Myers, *Conceptual Problems in the Use of Risk-Adjusted Discount Rates*, 21 J. FIN. 727, 727–30 (1966).

and U is the opportunity cost of the IP owner. The licensee pays compensation R that represents the present value of the expected stream of royalty payments to the IP owner, which is less than the benefit of the licensee and greater than the opportunity cost to the IP owner. License royalties divide gains from trade $V - U$.

Expectation damages for breach of a patent license contract are based on the royalties that the licensor would have received had the contract been honored by the licensee. Expectation damages for breach of contract generally protect the plaintiff's expectation.¹⁰⁵ Economic analysis suggests that expectation damages for breach of contract generate efficient performance decisions and also induce efficient reliance investment.¹⁰⁶

By protecting expectation interests, an IC provides incentives to invest efficiently in invention, innovation, and adoption. Expectation damages provide incentives for efficient investment in developing the invention and in complementary assets as well. This is because parties choose investment levels that maximize expected returns net of the costs of investment. Maximization of expected returns net of the costs of investment means that investment is chosen such that the expected marginal return to investment equals the marginal cost of investment. With only partial protections for expectation interests, a party to the contract may not receive all of the expected returns to investment. This implies that a party to the contract may not receive the expected marginal returns to additional investment. This provides incentives for a contracting party to choose an amount of investment below the efficient level. Consequently, a contracting party would not choose an amount of investment that maximizes expected returns net of the costs of investment. So, protection of expectation interests is necessary for parties to obtain the greatest possible gains from trade. ICs thus provide dynamic

105. See Charles J. Goetz & Robert E. Scott, *Liquidated Damages, Penalties and the Just Compensation Principle: Some Notes on an Enforcement Model and a Theory of Efficient Breach*, 77 COLUM. L. REV. 554, 562 n.32 (1977); Ian R. Macneil, *Contracts: Adjustment of Long-Term Economic Relations Under Classical, Neoclassical, and Relational Contract Law*, 72 NW. U. L. REV. 854, 864 n.31 (1978); Anthony T. Kronman, *Specific Performance*, 45 U. CHI. L. REV. 351, 352 (1978); Alan Schwartz, *The Case for Specific Performance*, 89 YALE L.J. 271, 271 (1979); Richard Craswell, *Contract Remedies, Renegotiation, and the Theory of Efficient Breach*, 61 S. CAL. L. REV. 629, 630 (1988).

106. See E. Allan Farnsworth, *Legal Remedies for Breach of Contract*, 70 COLUM. L. REV. 1145, 1147 (1970); John H. Barton, *The Economic Basis of Damages for Breach of Contract*, 1 J. LEGAL STUD. 277, 278 (1972); Robert L. Birmingham, *Breach of Contract, Damage Measures, and Economic Efficiency*, 24 RUTGERS L. REV. 273, 286 (1970); Lewis A. Kornhauser, *An Introduction to the Economic Analysis of Contract Remedies*, 57 U. COLO. L. REV. 683, 720–21 (1986); William P. Rogerson, *Efficient Reliance and Damage Measures for Breach of Contract*, 15 RAND J. ECON. 39, 44 (1984).

efficiencies that protect and increase benefits to inventors, innovators, and adopters.

IC rules are consistent with property protections for intangible assets. There are two main forms of legal protection for patent holders. Federal law protects the patent holder from infringement of IP rights by enforcing exclusion.¹⁰⁷ State law protects patent holders from infringement that results from breach of contract.¹⁰⁸ Phillip Jones points out that “the licensor may have the option to seek a remedy for a license restriction breach under the contract or from a patent infringement suit.”¹⁰⁹ Jones concludes that “[i]n fact, a licensor may be able to obtain the same range of remedies in state court for the breach of a license agreement that the licensor would be able to obtain in federal court for patent infringement under 35 U.S.C. §§ 283–85 (i.e., an injunction, compensatory damages, and attorney fees).”¹¹⁰

To illustrate how expectation damages affect breach decisions in patent license contracts, suppose that a licensor expects to receive a payment of R from the licensing agreement. For ease of discussion, suppose that the licensor does not have any lost profits and does not incur any licensing costs, although the discussion can readily be generalized without changing the conclusions. Expectation damages for a licensee breach of contract restore the licensor to the position he would be if the contract had been honored. This implies that damages D equal the payment R that the licensor would have received.

The damages remedy affects the licensee’s contract breach decision. Suppose that after the licensing contract is signed, the licensee develops an alternative invention that generates net benefits Z . Alternatively, Z could represent the market value of a new alternative invention net of royalty payments. The licensee will breach the contract if and only if the benefits of switching to the alternative technology net of switching costs and contract damages are greater than the net benefits of honoring the contract. This means that breach occurs if and only if the benefits of adopting the new technology net of damages $Z - D$ are greater than the benefits $V - R$ of the patented technology net of royalties.

Expectation damages equal the payment that the licensor expected to receive. Netting out the damage payment and the corresponding royalty payment, this implies that breach occurs if and only if the value Z obtained from applying the alternative technology is greater than the value V from the patented invention. This means that with expectation

107. 35 U.S.C. § 154 (2018).

108. Phillip B.C. Jones, *Violation of a Patent License Restriction: Breach of Contract or Patent Infringement?*, 33 IDEA: J.L. & TECH. 225, 226 (1993) (“[A] patent licensing agreement is a contract which is governed by principles of state contract law.”).

109. *Id.*

110. *Id.* at 240, n.75.

damages, breach of the licensing contract should occur if and only if breach is efficient, that is, if Z is greater than V . So, expectation damages for breach of licensing agreements provide incentives for efficient technology adoption decisions.

When expectation damages are sufficient to protect the expectation interests of the parties, the parties choose the terms of the agreement to maximize the present value of expected benefits. Also, the parties choose their investments to maximize the present value of total expected benefits. In this way, an IC increases the benefits of IP owners in comparison with immediate exchange and own use alone.

D. ICs and the Nature of the Firm

ICs are critical building blocks in the formation of innovative firms. ICs are essential to the “creative destruction” that takes place when innovative entrants compete with incumbent firms. Innovative firms contract with specialized researchers within the firm to develop and manage intangible assets. Innovative firms contract in the market with firms that create, own, or apply intangible assets. Innovative firms use ICs with customers, suppliers, partners, and distributors to introduce new products, production processes, transaction methods, and organizational structures. Innovative firms use ICs to provide multi-sided platforms that offer marketmaking and intermediary services to customers and suppliers.

Contracts are central to the formation of firms. The firm involves both internal and external contractual relationships.¹¹¹ The firm’s collection of internal and external contracts depends on the relative efficiency and transaction costs of these types of contracts. Steven Cheung interprets Ronald Coase’s analysis of the firm in terms of contract: “It is not quite correct to say that a ‘firm’ supersedes ‘the market.’ Rather, one type of contract supersedes another type.”¹¹²

A major purpose of the firm is to organize and manage the market for contracts. In my book *The Theory of the Firm*, I show that “[t]he firm is

111. Michael C. Jensen & William H. Meckling, *The Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure*, 3 J. FIN. ECON. 305, 310 (1976) (“[Firms] serve as a nexus for a set of contracting relationships among individuals.”); see Melvin A. Eisenberg, *The Conception that the Corporation Is a Nexus of Contracts, and the Dual Nature of the Firm*, 24 J. CORP. L. 819, 828 (1998).

112. Steven N.S. Cheung, *The Contractual Nature of the Firm*, 26 J.L. & ECON. 1, 10 (1983). Cheung states that an input owner has the option of own-use, selling the input to others, or creating a firm through contracts delegating the use of the input: “The firm emerges with the third option: the entrepreneur or the agent who holds a limited set of use rights by contract directs production activities without immediate reference to the price of each activity, and the commodities so produced are then sold in the market.” *Id.* at 3. See also Ronald Coase, *The Nature of the Firm*, 16 ECONOMICA 386 (1937).

an intermediary in the market for contracts.”¹¹³ Entrepreneurs establish firms when the benefits of intermediated contracts exceed the benefits of direct exchange: “Firms offer advantages over bilateral contracts through market making and coordination across multiple contracts.”¹¹⁴

IC relationships are essential to the creation of new types of firms. As I discuss in my book *The Innovative Entrepreneur*, entrepreneurs innovate to overcome the innovative inertia of incumbent firms.¹¹⁵ Entrepreneurs also innovate to overcome friction in the market for inventions that limit transfers of their technology to incumbent firms.¹¹⁶ Innovative entrepreneurs develop a complex set of contractual relationships, necessarily including ICs, to create startups and establish firms.

Contracts have well-known transaction costs, including the costs of search, negotiation, moral hazard, adverse selection, monitoring performance, and enforcement of contract terms. ICs have additional transaction costs, including difficulties in pricing IP and the costs of bundling IP with other goods and services.¹¹⁷ Because of the fundamental uncertainty involved in technological change, ICs have additional costs of forming contingent agreements and monitoring outcomes. Uncertainty associated with invention, innovation, and adoption is likely to be much greater than with contracts involving tangible assets.¹¹⁸

The firm’s outsourcing decisions concerning invention and innovation also depend on the relative costs of forming and monitoring an employment IC versus an outsourcing IC. The trade-off between governance costs and market transaction costs for ICs is related to Coase’s analysis of the scope of the firm’s activities and the make-or-buy decision.¹¹⁹ Coase’s analysis applied to technological change suggests that the firm will expand its inventive and innovative activities as long as

113. See DANIEL F. SPULBER, *THE THEORY OF THE FIRM: MICROECONOMICS WITH ENDOGENOUS ENTREPRENEURS, FIRMS, MARKETS, AND ORGANIZATIONS* 415 (2009).

114. *Id.*

115. See generally SPULBER, *supra* note 86.

116. *Id.*

117. See Richard Zeckhauser, *The Challenge of Contracting for Technological Information*, 93 PROC. NAT’L ACAD. SCI. U.S. 12473, 12473 (1996) (“Contracting to provide technological information (TI) is a significant challenge. TI is an unusual commodity in five ways. (i) TI is difficult to count and value; conventional indicators, such as patents and citations, hardly indicate value. TI is often sold at different prices to different parties. (ii) To value TI, it may be necessary to ‘give away the secret.’ This danger, despite nondisclosure agreements, inhibits efforts to market TI. (iii) To prove its value, TI is often bundled into complete products, such as a computer chip or pharmaceutical product. Efficient exchange, by contrast, would involve merely the raw information. (iv) Sellers’ superior knowledge about TI’s value make buyers wary of overpaying. (v) Inefficient contracts are often designed to secure rents from TI.”).

118. See discussion *infra* Section IV.

119. See generally Coase, *supra* 112.

incremental governance costs are less than the transaction costs of outsourcing these activities.¹²⁰

The trade-off between governance costs and transaction costs has important implications for innovative firms. The use of ICs both within the firm and among firms affects the direction of technological change. The reductions in the extent of vertical integration of the firm affect how R&D is organized in the economy. This is reflected in the design of products and production processes. Firms have reduced vertical integration by creating modular products and outsourcing contracts for innovation.¹²¹

The increasing importance of invention and innovation requires new types of intangible assets and organizations.¹²² Implementing technological change requires contractual agreements. Connecting individuals and firms in new ways requires more than networks of innovative technologies with digital links; it is also necessary to connect individuals and firms with networks of contracts that support the formation of these new technological networks. Individuals and firms need legal agreements for cooperative development of virtual inventions and innovations, and to help develop interconnectivity and interoperability of technologies. Individuals and firms also need contracts that support data sharing and investment in data gathering and analytics.

Technological change leading to vertical disintegration requires coordination through ICs between many vertical levels of suppliers. Various technological developments cut across industries, leading to greater reliance on outsourcing and licensing agreements. Technological changes that cross industries include AI, IoT, and ICT.¹²³

IC necessarily accompanies the growth of R&D outsourcing and the formation of innovation networks. Firms substitute networks of contracts

120. *Id.*

121. See Timothy J. Sturgeon, *Modular Production Networks: A New American Model of Industrial Organization*, 11 *INDUS. & CORP. CHANGE* 451, 451 (2002); Carliss Y. Baldwin, *Where Do Transactions Come From? Modularity, Transactions, and the Boundaries of Firms*, 17 *INDUS. & CORP. CHANGE* 155, 161 (2007); Ronald J. Gilson et al., *Contracting for Innovation: Vertical Disintegration and Interfirm Collaboration*, 109 *COLUM. L. REV.* 431, 435 (2009) (“Contracting for innovation supports iterative collaboration between firms by interweaving explicit and implicit terms that respond to the uncertainty inherent in the innovation process . . .”); Margaret M. Blair et al., *Outsourcing, Modularity, and the Theory of the Firm*, *BYU L. REV.* 263, 265–66 (2011).

122. Erik Brynjolfsson et al., *Intangible Assets: Computers and Organizational Capital*, 1 *BROOKINGS PAPERS ON ECON. ACTIVITY* 137, 138 (2002) (“This paper analytically explores the hypothesis that new, intangible organizational assets complement [information technology] capital just as new production processes and factory redesign complemented the adoption of electric motors over 100 years ago.”).

123. Kay Firth-Butterfield & Yoon Chae, *Artificial Intelligence Collides with Patent Law*, *CTR. FOR THE FOURTH INDUS. REVOLUTION* 3, 5 (Apr. 2018) http://www3.weforum.org/docs/WEF_48540_WP_End_of_Innovation_Protecting_Patent_Law.pdf.

for vertical integration.¹²⁴ Contracts among firms substitute for contracts within the firm. Matthew Jennejohn observes, “[w]here property rights no longer control, contracts substitute. In light of these developments, contract’s place as one of capitalism’s fundamental building-blocks takes on even greater importance.”¹²⁵

Many types of invention and innovation require coordination of activities across firms. This is reflected in the increasing importance of technological standards. There are over one thousand standard setting organizations (SSOs) that establish quality and interoperability standards in practically every industry.¹²⁶ Changes in technology standards provide an important indication of innovation.¹²⁷ Standards include “variety control, usability, compatibility, interchangeability, health, safety, protection of the environment, product protection, mutual understanding, economic performance, trade.”¹²⁸ For example, the International Organization for Standardization (ISO) has published over 21,000 international standards,¹²⁹ playing an important role in the formation of global supply chains. The management literature refers to the extensive technological interdependence among firms as innovative “ecosystems.”¹³⁰

II. INTELLECTUAL CONTRACT

Intellectual Law offers a framework for addressing intangible assets in a comprehensive manner. This section examines some of the main differences between ICs and standard contracts; it also sets out five basic principles of IC law. IC involves agreements that resolve some of the incompleteness of IP. IC also helps remedy difficulties in exclusion of access to intangible assets. IC provides agreements when there is non-rivalrous usage of intangible assets. IC provides incentives for

124. Matthew C. Jennejohn, *Collaboration, Innovation, and Contract Design*, 14 STAN. J. L., BUS. & FIN. 83, 84 (2008) (“Rather, deverticalized firms enmesh themselves in webs of collaboration—joint ventures, strategic alliances, just-in-time (JIT) production arrangements, etc.—usually in hope of cost-cutting but also with an eye to securing competitive advantage through innovation.”).

125. *Id.*

126. Daniel F. Spulber, *Standard Setting Organizations and Standard Essential Patents: Voting and Markets* 2 ECON. J., (forthcoming, Apr. 2019), <https://doi.org/10.1111/econj.12606>.

127. *Id.*

128. ISO/IEC GUIDE 2:2004 at 12 (INT’L ORG. FOR STANDARDIZATION & INT’L ELECTROTECHNICAL COMM’N 2004), <https://www.iso.org/obp/ui/#iso:std:iso-iec:guide:2:ed-8:v1:en>.

129. INT’L ORG. FOR STANDARDIZATION, NAVIGATING A WORLD IN TRANSITION 35 (2016), https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/annual_reports/en/annual_report_2016_en.pdf.

130. See generally Ron Adner & Rahul Kapoor, *Value Creation in Innovation Ecosystems: How the Structure of Technological Interdependence Affects Firm Performance in New Technology Generations*, 31 STRATEGIC MGMT. J. 306 (2010).

exploratory performance. Finally, IC addresses problems of contingent contracting when agreements are subject to fundamental uncertainty.

A. ICs and Incompleteness of IP

IP suffers from weak enforcement as well as the inherent limitations of government grants and registration. A well-functioning system of property rights requires completeness, exclusivity, and transferability. ICs provide protections for intangible assets based on agreements between inventors, innovators, and adopters. This compensates for incompleteness of legal protections for intangible assets. An advantage of ICs is that they do not require government approval of the IP defined through the agreement. The transaction costs of IC are likely to be substantially lower than costs associated with government administration. Contractually-defined protections are tailored to the particular benefits and costs of the contracting parties and the characteristics of the technology.

The Constitution frames protections for inventors in terms of IP by giving Congress the power to secure exclusive rights for authors and inventors to their writings and discoveries.¹³¹ Patent holders have the right to exclude others from making, using, offering to sell, selling, or importing any patented invention.¹³² State governments and all three branches of the federal government are involved in defining and enforcing IP rights.¹³³ IP policies include legislative limitations on IP, executive policies toward IP—particularly involving the USPTO and antitrust agencies—and judicial decisions on IP. Many practitioners and scholars emphasize the importance of IP protections for inventors.¹³⁴

IP protections for commercial, scientific, and technological creations are far from complete however. IP provides protections in four categories: patents, trademarks, copyrights, and trade secrets.¹³⁵ The

131. U.S. CONST. art. I, § 8, cl. 8 (“The Congress shall have Power . . . 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”). See also Gene Quinn, *Patents, Copyrights and the Constitution, Perfect Together*, IPWATCHDOG (Feb. 19, 2018), <http://www.ipwatchdog.com/2018/02/19/patents-copyrights-constitution/id=93941/>.

132. See 35 U.S.C. § 271 (2018).

133. *Id.*; see also Fla. Stat. § 815.04 (2018).

134. See, e.g., Roger D. Blair & Thomas F. Cotter, *An Economic Analysis of Damages Rules in Intellectual Property Law*, 39 WM. & MARY L. REV. 1585, 1615 (1997) (“A substantial number of the law and economics scholars who have written on this subject appear to agree that it is generally preferable to protect intellectual property rights through the use of property, as opposed to liability, rules.”).

135. *Trade Secret Policy*, USPTO, <https://www.uspto.gov/patents-getting-started/international-protection/trade-secret-policy> (last visited Nov. 24, 2018). But see WORLD INTELLECTUAL PROP. ORG., WHAT IS INTELLECTUAL PROPERTY? (2003) <http://www.wipo.int/>

WIPO Convention's definition of IP is more inclusive because it identifies "scientific discoveries" and "all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields."¹³⁶

In contrast to tangible property, patents and trademarks require government grants.¹³⁷ The USPTO not only registers the property right, but defines and certifies the features of the intangible asset.¹³⁸ At the USPTO, professional patent examiners review applications for patents and examining attorneys review applications for trademarks.¹³⁹ For inventions to be "patentable," they must satisfy criteria such as first-to-file, novelty, and non-obviousness.¹⁴⁰ For trademarks to be "registrable," there cannot be a "likelihood of confusion" with existing trademarks or pending applications.¹⁴¹ The chance that a trademark is "registrable" also depends on the category it belongs to: fanciful or arbitrary, suggestive, descriptive, or generic.¹⁴²

There are also limitations for copyright. In fiscal year 2016, the U.S. Copyright Office issued over 414,000 registrations out of 468,000 claims for registration.¹⁴³ The U.S. Copyright Office limits types of works and applies subject matter criteria, governed by statute: "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle,

edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf; WORLD INTELLECTUAL PROP. ORG., INTELLECTUAL PROPERTY HANDBOOK 3 (2d ed. 2004), http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf ("Generally speaking, intellectual property law aims at safeguarding creators and other producers of intellectual goods and services by granting them certain time-limited rights to control the use made of those productions. Those rights do not apply to the physical object in which the creation may be embodied but instead to the intellectual creation as such. Intellectual property is traditionally divided into two branches, 'industrial property' and 'copyright.'").

136. Convention Establishing the World Intellectual Property Organization art. 2, July 14, 1967, 21 U.S.T. 1749, 828 U.N.T.S. 3.

137. Gene Quinn, *SCOTUS Says Patents Are a Government Franchise, Not a Vested Property Right*, IPWATCHDOG (Apr. 24, 2018), <https://www.ipwatchdog.com/2018/04/24/scotus-says-patents-government-franchise-not-vested-property-right/id=96324/>; see also *Oil States Energy Servs., LLC v. Greene's Energy Grp., LLC*, 138 S. Ct. 1365, 1373 (2018).

138. See 35 U.S.C. § 2(a) (2018).

139. See 35 U.S.C. § 131 (2018); 15 U.S.C. § 1051 (2018).

140. See 35 U.S.C. §§ 100–03 (2018).

141. USPTO, PROTECTING YOUR TRADEMARK: ENHANCING YOUR RIGHTS THROUGH FEDERAL REGISTRATION 3 (2016), <https://www.uspto.gov/sites/default/files/documents/BasicFacts.pdf>.

142. *Id.* at 7.

143. *Overview of the Copyright Office*, U.S. COPYRIGHT OFFICE, <https://www.copyright.gov/about/> (last visited Jan. 21, 2019).

or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.”¹⁴⁴

IP offers weaker protections for inventors than protections for traditional property rights. In contrast to tangible property, patents limit the time period of exclusive rights. The regulatory time limit is a form of incompleteness. Richard Epstein argues that limiting the time period of exclusive rights transforms tangible property rules to intangible property rules.¹⁴⁵ Epstein suggests that limiting the time period for exclusion, use, and disposition is similar to other limits placed on property generally, including the law of private and public necessity and antitrust limitations on collusion.¹⁴⁶

Subject matter limitations are another major form of incompleteness for IP.¹⁴⁷ The subject matter limitations for patentability under the statute specify “any new and useful process, machine, manufacture, or composition of matter.”¹⁴⁸ The Supreme Court in *Bilski* questioned whether business method inventions should be patentable.¹⁴⁹ The decision cast doubt on many existing business method patents and the full range of commercial inventions, including Internet commerce software applications.¹⁵⁰ The Supreme Court decision in *Mayo* raised issues about biotechnology inventions by diagnostic tests for administering pharmaceuticals.¹⁵¹ The Court rejected the invention using a two-step test that first determined whether the invention consisted of “abstract ideas, laws of nature, or natural phenomena,” then examined whether the invention would “transform the nature of the claim” into something

144. 17 U.S.C. § 102 (2018).

145. Richard A. Epstein, *The Disintegration of Intellectual Property? A Classical Liberal Response to a Premature Obituary*, 62 STAN. L. REV. 455, 459 (2010) (“As I shall argue, the single adoption of one adjustment, and one adjustment only, goes a very long way to ease the transformation from tangible to intangible property. Just use limited terms of exclusive rights, longer for copyrights than patents, to work the transformation from tangible property to these two vital forms of intellectual property. At that point, the remainder of the rules that deal with tangible property, namely those that concern exclusion, use, and disposition, can be carried over without difficulty.”).

146. *Id.*

147. USPTO, PATENT ELIGIBLE SUBJECT MATTER: REPORT ON VIEWS AND RECOMMENDATIONS FROM THE PUBLIC UNITED STATES PATENT AND TRADEMARK OFFICE (2017), https://www.uspto.gov/sites/default/files/documents/101-Report_FINAL.pdf.

148. 35 U.S.C. § 101 (2018).

149. *Bilski v. Kappos*, 561 U.S. 593 (2010).

150. *Id.*; see also Daniel F. Spulber, *Should Business Method Inventions Be Patentable?*, 3 J. LEGAL ANALYSIS 265, 267 (2011).

151. *Mayo v. Prometheus*, 132 S. Ct. 1289 (2012).

patentable.¹⁵² The Supreme Court applied the two-step test in *Alice* to reject a business invention for intermediated settlement.¹⁵³

IP also provides incomplete protections because patents do not cover many incremental inventions.¹⁵⁴ The costs and difficulties in obtaining and maintaining a patent can be very high.¹⁵⁵ This inevitably generates an expected value threshold for patent protections. An inventor will not apply for a patent unless the expected value of patenting the invention exceeds the costs of obtaining the patent. Consequently, patent protections are incomplete because they do not cover inventions with expected values below the threshold.

ICs help protect discoveries in the lower tail of the distribution of the market value of inventions. IP tends to cover the upper tail of inventions and other intangible assets.¹⁵⁶ Let C represent the expected legal costs and fees of obtaining and maintaining IP such as patents. Let Y be the market value of the IP, including own use by the IP holder, if found to be valid by the courts. Let P be the likelihood that IP is found to be valid by the courts and survives administrative challenges. Then, it is not worthwhile obtaining IP if the expected benefits PY are less than the expected costs C . This type of IP is the lower tail of the net value distribution of intangible assets. Yet, incremental discoveries are generated routinely and are highly important within the firm. There are many discoveries in the lower tail of the distribution of the market value of inventions.¹⁵⁷

In addition, patent application criteria and uncertainty in review by patent examiners limit coverage for inventors. Many discoveries may be original but not meet formal IP criteria, including those based on laws of

152. USPTO, *supra* note 147, at 8.

153. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).

154. Gene Quinn, *Protecting Ideas: Can Ideas Be Protected or Patented?*, IP WATCHDOG (Feb. 15, 2014), <http://www.ipwatchdog.com/2014/02/15/protecting-ideas-can-ideas-be-protected-or-patented/id=48009/>.

155. Quinn, *supra* note 29 (“Thanks to the United States Supreme Court, the United States Court of Appeals for the Federal Circuit and ever more regulations from the United States Patent and Trademark Office it has become more difficult over the years to create the type of written description and claim sets required.”).

156. Jill Green & Melody Wirz, *Whose Idea Is it Anyway? 10 IP Issues in Deals*, ACC DOCKET, Dec. 2010, at 40.

157. See Bronwyn H. Hall and Rosemarie H. Ziedonis, *The Patent Paradox Revisited: An Empirical Study of Patenting in the US Semiconductor Industry, 1979-1995*, 32 RAND J. ECON., 101 (2001); Lee Fleming, *Breakthroughs and the “Long Tail” of Innovation*, 49 MIT SLOAN MGMT. REV. 69 (2007); Cédric Schneider, *External Knowledge Sourcing: Science, Market and the Value of Patented Inventions*, 30 MANAGERIAL AND DECISION ECON. 551 (2009); and Gaétan De Rassenfosse, *Do Firms face a Trade-Off between the Quantity and the Quality of their Inventions?*, 42 RESEARCH POLICY 1072 (2013).

nature, non-obviousness, and usefulness.¹⁵⁸ These considerations eliminate property protections for inventions that do not pass through formal review and meet the regulatory criteria. The risks of the review process further increase the expected value threshold for patent protections.¹⁵⁹ Fewer inventors seeking patent protections which further increases the incompleteness of IP.

IP protections also are incomplete because of costs and inaccuracies in the legal and regulatory systems. Patent holders face costs of detecting and monitoring infringement.¹⁶⁰ The legal costs of obtaining compensation for infringement are significant. Additionally, patents are subject to costly legal challenges in terms of validity and infringement. Unavoidable legal errors, inconsistencies, and technical issues further limit IP protections for some useful and original inventions. Patents are also subject to challenge at the Patent Trial and Appeal Board (PTAB) within the USPTO, which may also be subject to error.¹⁶¹ Taken together, these costs and risks create another type of value threshold for patent protections. Patents with an expected value below this threshold will not have IP protections.

Stronger protections for trade secrets address some of these limitations. More companies rely on protections from trade secrets and trademarks than from copyrights and patents.¹⁶² Trade secrets do not require formal government grants of IP.¹⁶³ Ivan Png points out that “trade

158. Gene Quinn, *Patentability: The Nonobviousness Requirement of 35 U.S.C. 103*, IP WATCHDOG (June 17, 2017), <http://www.ipwatchdog.com/2017/06/17/patentability-nonobviousness-35-usc-103/id=84716/>.

159. Neal Solomon, *The Problem of Patent Valuation*, IP WATCHDOG (Aug. 15, 2017), <http://www.ipwatchdog.com/2017/08/15/problem-patent-valuation/id=86840/>.

160. Rebecca S. Eisenberg, *Patent Costs and Unlicensed Use of Patented Inventions*, 78 U. CHI. L. REV. 53, 54–55 (2011).

161. Gene Quinn, *PTAB Judges Shockingly Inexperienced Compared to District Court Judges*, IP WATCHDOG (Mar. 6, 2018), <http://www.ipwatchdog.com/2018/03/06/ptab-judges-shockingly-inexperienced/id=94438/> (“The America Invents Act (AIA) invests PTAB judges with extraordinary powers. For example, overwhelmingly institution decisions are not appealable. Yet, there have been numerous lawyers with shockingly little experience appointed to the position of patent judge, and vested with the power to make decisions that cannot be reviewed by any Article III federal court.”).

162. See JOHN E. JANKOWSKI, NAT’L SCI. FOUND., BUSINESS USE OF INTELLECTUAL PROPERTY PROTECTION DOCUMENTED IN NSF SURVEY 1 (2012), <http://wayback.archive-it.org/5902/20181004073804/https://www.nsf.gov/statistics/infbrief/nsf12307/nsf12307.pdf> (“New survey findings from the National Science Foundation (NSF) and the U.S. Census Bureau (Census) indicate that trademarks and trade secrets are identified by the largest number of businesses as important forms of IP protection, followed by copyrights, and then patents.”); see generally JAMES POOLEY, TRADE SECRETS (2017).

163. Shane E. Olafson, *Patents vs. Trade Secrets—Giving Your Business the Competitive Edge*, ARIZ. BIOINSIDER (Apr. 1, 2007), https://www.lrrc.com/files/Uploads/Documents/Olafson_AZBioInsider.pdf.

secrets can be unlimited in time, are not limited by particular technical standards, and do not require disclosure. Moreover, the scope of trade secrecy is much broader, extending to work in progress as well as completed innovations.”¹⁶⁴ Individual states’ adoption of the Uniform Trade Secrets Act (UTSA) has increased protections for inventors and innovators.¹⁶⁵ Png finds that state adoption of the UTSA has tended to increase R&D.¹⁶⁶

Although trade secrets cover works in progress, they are not sufficient to protect the continual sharing of information within and among firms. Many lower tail discoveries must be disclosed to employees and the firm’s customers, suppliers, and partners.¹⁶⁷ ICs overcome some of the limitations of trade secret protections. IC protections, such as non-disclosure agreements (NDAs), address the need to share various trade secrets in employment and outsourcing.¹⁶⁸

ICs help protect cooperative use of knowledge and intangible assets not covered by formal IP. Technological change involves repeated interactions over time between a firm and its employees and among firms. This interaction involves continual sharing of small increments of knowledge. The formal apparatus of IP cannot protect such small increments of knowledge because IP is geared to larger increases in knowledge. This is because the sharing of small increments of knowledge is often informal and incomplete. Also, the costs of obtaining government grants of IP are necessarily prohibitive for small increments of knowledge. Continual sharing of knowledge may involve relational contracts because of the need for trust and implicit agreements that cannot be achieved with IP.

B. ICs and Excludability of IP

Parties can form ICs to allocate ownership of intangible assets and to specify how those assets will be used. These private agreements depend on contract rules and private negotiation. ICs resolve problems related to the excludability of intangible assets. The parties to an IC can choose the

164. I.P.L. Png, *Law and Innovation: Evidence from State Trade Secrets Laws*, 99 REV. ECON. & STAT. 167, 168 (2017).

165. *Id.* at 175.

166. *Id.*

167. Evelyn D. Pisegna-Cook, *Ownership Rights of Employee Inventions: The Role of Preinvention Assignment Agreements and State Statutes*, 2 U. BALT. INTELL. PROP. L.J. 163, 163 (1994).

168. Epstein, *supra* note 145, at 458 (“Any agreement, for example, whereby a trade secret is shared pursuant to a confidentiality agreement involves the simultaneous transmission and retention of information—but only if the contractual arrangements are given strong protection, as they typically are.”).

desired extent of exclusion. The effectiveness of IP should be considered in combination with ICs.

Legal barriers limiting access to IP substitute for the lack of physical barriers. It is more difficult for IP owners to limit, deter, and monitor access to intangible assets in contrast to tangible assets.¹⁶⁹ Peter Menell notes that “even if someone claims to own the knowledge, it is difficult to exclude others from using it. Intellectual property law is an attempt to solve that problem by legal means.”¹⁷⁰ R&D can generate positive externalities because knowledge can be costless for others to learn and distribute while it can be costly for IP holders to monitor usage by others. Positive externalities from R&D often are referred to as R&D “spillovers.”¹⁷¹

The debate over patent scope considers the effects of legal exclusion on sequential invention and innovation. Robert Merges and Richard Nelson argue that patent scope should be narrow so as to encourage rivalry among inventors.¹⁷² They express concerns that narrow patents will favor pioneer inventors and block competing inventors.¹⁷³ Advocates of narrow patent scope argue that exclusion creates monopoly rents for patent holders.¹⁷⁴ The advantages of not protecting patent holders’ investments in developing an invention are inducing investment in developing and applying the invention by later inventors.¹⁷⁵

Others argue that patent scope should be sufficiently broad to help inventors develop their own inventions without incursion by later inventors.¹⁷⁶ Broader patent protections encompassing future development encourage inventors to invest in improving and

169. Owners of buildings and land can place fences around their properties. Owners of automobiles and other vehicles can equip them with locks and other antitheft devices. Companies have various mechanisms for deterring theft of their goods, equipment, and financial assets.

170. Menell, *supra* note 31, at 726.

171. Pere Arqu -Castells & Daniel F. Spulber, *Measuring the Private and Social Returns to R&D: Unintended Spillovers Versus Technology Markets* (Nw. L. & Econ. Research, Paper No. 18-18, 2019), <http://dx.doi.org/10.2139/ssrn.3202870>.

172. See Robert P. Merges & Richard R. Nelson, *On the Complex Economics of Patent Scope*, 90 COLUM. L. REV. 839 (1990); Robert P. Merges & Richard R. Nelson, *On Limiting or Encouraging Rivalry in Technical Progress: The Effect of Patent Scope Decisions*, 25 J. ECON. BEHAV. & ORG. 1, 6 (1994).

173. See sources cited *supra* note 172.

174. Michele Boldrin & David K. Levine, *The Case Against Patents*, 27 J. ECON. PERSP. 3, 18 (2013).

175. See Suzanne Scotchmer, *Standing on the Shoulders of Giants: Cumulative Research and the Patent Law*, 5 J. ECON. PERSP. 29, 30 (1991).

176. On arguments for broader patent scope, see Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265 (1977); Daniel F. Spulber, *How Patents Provide the Foundation of the Market for Inventions*, 11 J. COMP. L. & ECON. 271 (2015).

commercializing their patented inventions.¹⁷⁷ Broader patent protections also support investment in creating the initial invention and encourage disclosure of inventions.¹⁷⁸ Also, broader patent protections allow patent holders to choose the mix of own use and outsourcing efficiently based on the relative economic returns to these activities.

With positive externalities from R&D, the social benefits of the initial invention are greater than the private benefits to the initial inventor. With broader patent scope, there is greater protection for IP rights of inventors and correspondingly fewer R&D spillovers. Conversely, with narrower patent scope, there is less protection for IP rights of inventors and correspondingly more R&D spillovers.

The problem of patent scope is thus similar to the problem of social cost. The social costs of an activity are defined as the total of private costs.¹⁷⁹ The social costs of an activity exceed the private costs to the owner of an activity when the activity imposes costs on others.¹⁸⁰ The costs or harm imposed on others are referred to as a negative externality if the costs are not part of a market transaction between the parties. Coase showed that private negotiation achieves efficiency regarding the extent of negative externalities when transaction costs are low and few parties are involved.¹⁸¹ Coase emphasized that the assignment of property rights does not affect the efficiency of the outcome because the negotiating parties maximize their joint benefits.¹⁸² If the party creating harm has property rights, the party suffering harm will pay them to stop.¹⁸³ If the party suffering harm has property rights, the party creating harm will be forced to pay compensation.¹⁸⁴ The extent of the activity will be such that the marginal private benefit to the party causing harm will equal the marginal damage to the party suffering harm.¹⁸⁵ The only effect of the initial assignment of property rights is distributional because the party with property rights will benefit at the expense of the party without property rights.¹⁸⁶

When transaction costs are low and few parties are involved, the parties are able to attain an efficient outcome regardless of the assignment of property rights.¹⁸⁷ However, when transaction costs are high and many

177. Kieff, *supra* note 92, at 710.

178. Kitch, *supra* note 176, at 278.

179. ARTHUR CECIL PIGOU, *THE ECONOMICS OF WELFARE* 189 (4th ed. 1932).

180. *Id.*

181. Ronald H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

182. *Id.* at 6.

183. *Id.* at 9.

184. *Id.*

185. *Id.* at 3.

186. *Id.* at 5.

187. *Id.* at 6.

parties are involved, the assignment of property rights can affect the outcome.¹⁸⁸ This is because frictions may prevent or distort bargaining, thus preventing the parties from attaining an efficient outcome. It is then more efficient to assign property rights so as to minimize transaction costs. For example, there may be a few firms engaged in the activity that causes harm and many individuals suffering harm from the external effects of the activity. It is then more efficient to assign property rights to those suffering harm.

ICs can address the problem of patent scope and the effects of positive externalities from R&D. When transaction costs are low and few parties are involved, contract negotiation should attain the efficient outcome regardless of patent scope. If patent scope is narrow, the party benefitting from the initial invention can pay the inventor to conduct R&D. If patent scope is broad, the party benefitting from the initial invention can pay the inventor to use the invention, thus providing additional incentives for the inventor. The parties will reach an efficient agreement regardless of the initial assignment of IP rights.

ICs may not fully remedy the problem of patent scope when transaction costs are high and many parties are involved. In this situation, the choice of patent scope does affect economic efficiency. It is necessary for patent policy to assign property rights that achieve the right mix of initial and sequential invention. This suggests the need for broader patent scope because licensing the invention to later inventors should involve lower transaction costs than providing subsidies to potential initial inventors. As Merges points out, many potential buyers and high transaction costs suggest the need for stronger IP to support contracts.¹⁸⁹

The length of patent life affects the initial inventor's returns from transferring or licensing the patent to the second inventor.¹⁹⁰ Also, the scope of the patent affects the extent to which sequential invention requires the second inventor to acquire or license the intangible assets of

188. Harold Demsetz, *Information and Efficiency: Another Viewpoint*, 12 J.L. ECON. 1, 13 (1969) ("If the cost of contracting is positive, the kind of property rights system that is established may change the allocation of resources in the production of knowledge.").

189. Robert P. Merges, *Of Property Rules, Coase, and Intellectual Property*, 94 COLUM. L. REV. 2655, 2662 (1994) ("Even though there are many dispersed buyers (and sellers) of IPRs, and even though the transaction costs of IPR exchanges are otherwise high, the strong property rule baseline often works quite well. The frequency of contracting in many markets for IPRs—an underdeveloped theme in most of the entitlements literature—gives rise to a myriad of institutions (broadly defined) designed to streamline the exchange of property rights.").

190. See Jerry R. Green & Suzanne Scotchmer, *On the Division of Profit in Sequential Innovation*, 26 RAND J. ECON. 20, 21 (1995); Ted O'Donoghue et al., *Patent Breadth, Patent Life, and the Pace of Technological Progress*, 7 J. ECON. & MGMT. STRATEGY 1, 2 (1998); John H. Barton, *Patents and Antitrust: A Rethinking in Light of Patent Breadth and Sequential Innovation*, 65 ANTITRUST L.J. 449, 450 (1997).

the first inventor.¹⁹¹ ICs allow the allocation of returns among sequential inventors. Nancy Gallini argues that shorter lived, broad patents promote diffusion of inventions but longer lived, narrow patents lower R&D costs.¹⁹² Amy Landers recommends that in patent disputes, courts should consider sequential invention and defines apportionment as “an examination of the differences between the infringed claim and the prior art in a manner analogous to the identification of the differences between the claimed invention and the prior art in the non-obviousness analysis.”¹⁹³

ICs also provide an important mechanism for addressing positive externalities in R&D.¹⁹⁴ Firms can internalize these benefits through licensing or cross-licensing agreements. Firms also can internalize positive externalities by creating RJVs and R&D consortia. Companies forming RJVs may employ covenants not to compete (CNCs) to coordinate their R&D activities. This type of CNC is a form of IC. CNCs date back over three centuries.¹⁹⁵ Sarath Sanga points out that corporate joint ventures involve an inherent fiduciary conflict between each company’s duty to its own interests and its duty to the interests of a partner.¹⁹⁶ Sanga argues that this conflict of interests is resolved not only by operating the joint venture as a separate entity, but through the use of a CNC.¹⁹⁷

ICs address problems arising from insufficient exclusivity of IP. Firms must disclose IP within their organizations. Firms licensing IP must disclose the features of the invention. Kenneth Arrow observed that offering inventions for sale or license involves revealing the secret.¹⁹⁸ Inventors must disclose their technology in order to obtain a patent. Trademarks and copyrighted works only have value if used openly.

191. See O’Donoghue et al., *supra* note 190, at 2; Barton, *supra* note 190, at 449.

192. Nancy T. Gallini, *Patent Policy and Costly Imitation*, 23 RAND J. ECON. 52, 53 (1992).

193. Amy L. Landers, *Patent Claim Apportionment, Patentee Injury and Sequential Invention*, 19 GEO. MASON L. REV. 471, 476 (2012).

194. For some discussion of spillovers and RJVs, see Claude D’Aspremont & Alexis Jacquemin, *Cooperative and Noncooperative R&D in Duopoly with Spillovers*, 78 AM. ECON. REV. 1133 (1988); Kotaro Suzumura, *Cooperative and Noncooperative R&D in an Oligopoly with Spillovers*, 82 AM. ECON. REV. 1307 (1992).

195. Harlan M. Blake, *Employee Agreements Not to Compete*, 73 HARV. L. REV. 625, 629 (1960).

196. Sarath Sanga, *A Theory of Corporate Joint Ventures*, 106 CAL. L. REV. 1437, 1438 (2018).

197. *Id.* at 1454.

198. Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, 0-87014-304-2 NAT’L BUREAU OF ECON. RES. 609, 615 (1962), <https://www.nber.org/chapters/c2144.pdf>.

ICs also help control technology transactions that occur when employees who switch jobs convey knowledge and inventions from their previous employer to their new one. Ronald Gilson includes legal frameworks as a source of agglomeration economies driving places like California's Silicon Valley.¹⁹⁹ Gilson emphasizes the importance of CNCs that facilitate employee job switching while protecting a company's intangible assets.²⁰⁰ These types of CNCs also function as ICs.

Legal barriers provide weaker protections for intangible assets than for tangible assets. ICs remedy weaknesses in legal protections for IP. Infringement of a patent occurs when someone "without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent . . ."²⁰¹ An IC specifies who will make, use, offer to sell, or sell an invention, and places additional limitations on use and the amount of compensation. Enforcement of the agreement provides protections of the contracting parties' expectations.

C. ICs and Non-Rivalrous Usage of IP

Non-rivalrous usage of intangible assets distinguishes ICs from standard contracts involving tangible assets. ICs handle the non-rivalrous usage of intangible assets by facilitating allocation and sharing among multiple adopters. ICs support cooperation in developing and combining intangible assets. For example, a patent holder can grant access to an invention to multiple users by offering multiple patent license contracts.

ICs help define the characteristics and boundaries of intangible assets. Agreements between inventors, innovators, and adopters specify the features of technology being shared or transferred. Contracts adjust to the benefits and costs of the parties to the agreement and the needs of the industries in which they do business.

Some argue that IP should not receive the same legal protections as tangible property because of extensive interdependence associated with information. For example, Menell asserts: "Intellectual property has never fit the real property mold particularly well and the inherent attributes of intellectual resources as well as the increasingly interdependent nature of information ecosystems points away from the [property rights movement's] PRM's conception of property."²⁰²

199. Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575, 577 (1999).

200. *Id.*

201. 35 U.S.C. § 271 (2018).

202. Menell, *supra* note 31, at 753.

Yet, as Polk Wagner observes, even open source advocates seek control: “[D]espite rhetoric to the contrary, it seems quite clear that the ‘open’ in open source is actually rather tightly controlled, albeit in the name of generally greater access along certain philosophically-favored dimensions.”²⁰³ Polk points out that even open source advocates turn to contracts for coordination:

It should come as no surprise that participants in open source development efforts recognize the need for external coordination, chiefly attempting to accomplish this through the licensing of intellectual property rights to the software. Such licenses are not trivial; perhaps the best known open source license, the GNU General Public License (GPL), has been noted as an aggressive approach to both contract and copyright law, purporting to bind all subsequent users of the software to the terms of the original license.²⁰⁴

Transactions among inventors, innovators, and technology adopters depend on effective IC rules. ICs that protect the expectation interests of investors generate the benefits of interdependence in markets for invention. IP provides the foundation for the market for inventions.²⁰⁵ ICs realize the benefits of coordination among creators and IP users. ICs provide parties with mechanisms to benefit from non-rivalrous usage of intangible assets.

D. ICs and Incentives for Exploratory Performance

An IC must solve the critical problem of designing incentives for what I refer to as exploratory performance. With technological change, the characteristics of the outcomes of invention, innovation, and technology adoption are likely to be unknown. The uncertainty involved is more complex than a lottery over known outcomes.

Uncertainty about the characteristics of outcomes increases transaction costs of contracting.²⁰⁶ This distinguishes ICs from standard contracts involving tangible assets. Difficulties in specifying

203. R. Polk Wagner, *Information Wants to Be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995, 1031 (2003).

204. *Id.* at 1030.

205. Spulber, *supra* note 77, at 271.

206. On transaction costs of contract formation, see Coase, *supra* note 112, and Coase, *supra* note 181, at 15–16.

performance also will affect the incentives of parties involved in contract negotiation.²⁰⁷

An IC must specify the bargain when the characteristics of outcomes are unknown. With unknown outcomes, it becomes difficult to specify what performance is being offered and what performance is being accepted. The problems of defining and verifying performance make it difficult to determine the intent of the parties.

Almost all invention, innovation, and technology adoption involves delegation, whether it be to specialized personnel, managers, or firms.²⁰⁸ So, an IC is likely to be subject to the two main forms of agency costs resulting from moral hazard and adverse selection.²⁰⁹ A moral hazard problem arises when the employee's actions are imperfectly observable or verifiable.²¹⁰ Then, the IC must be based on some measure of performance generated by the employee's actions. Because there is a tradeoff between the cost of inducing action and the benefits of the action, the agent's action will differ from what would be chosen with observable actions.²¹¹ The agent may not choose an efficient level of effort or investment.²¹² Here, an efficient level of effort or investment refers to actions that maximize the joint benefits of the contracting parties. If the agent's activity is subject to additional uncertainty, it is not possible to infer the agent's effort from the resulting output. Contracts must therefore provide incentives to the agent or partner to generate effort or investment. Contractual incentives are based on the measure of performance and reward hidden actions indirectly.

An IC is also likely to be subject to adverse selection. An adverse selection problem arises if the employee has hidden information.²¹³ Even if the agent's action is observable and legally verifiable, the other party will not know what would have been the most efficient action. To address this problem, it is necessary to reward the agent's performance. There is

207. The costs and rules of contract formation affect the incentives of parties involved in contract negotiation, see Coase, *supra* note 181; Avery Katz, *The Strategic Structure of Offer and Acceptance: Game Theory and the Law of Contract Formation*, 89 MICH. L. REV. 215, 230 (1990).

208. Poblete & Spulber, *supra* note 39, at 39 ("Firms must design and apply incentive contracts for specialized economic agents who conduct R&D because most R&D is a delegated activity. The skills, knowledge and personnel necessary for the invention often differ from those needed for other production and operating activities and generally require independent business units. Companies and government agencies conduct R&D in-house by employing specialized experts such as scientists, engineers, and statisticians.").

209. Masako N. Darrough & Neal M. Stoughton, *Moral Hazard and Adverse Selection: The Question of Financial Structure*, 41 J. FIN. 501, 501 (1986).

210. *Id.*

211. Gustavo Manso, *Motivating Innovation*, 66 J. FIN. 1823, 1830 (2011).

212. Poblete & Spulber, *supra* note 39, at n.6.

213. Darrough & Stoughton, *supra* note 209, at 501.

a tradeoff between the cost of inducing the agent to tell the truth and benefits of obtaining an accurate report.²¹⁴ To induce truth telling, it may be necessary to allow a distortion of the agent's effort away from the efficient level of effort.²¹⁵

Contracting costs associated with exploratory performance may differ from the agency costs associated with moral hazard and adverse selection. An IC can address the problem of determining exploratory performance when there is a general measure of benefits for one of the parties.²¹⁶ For example, a firm can base the rewards for specialized R&D personnel on the overall performance of the firm. This can be achieved by providing stock options for both managers and specialized R&D personnel.²¹⁷ Software companies provide long-term incentive contracts, such as stock options, to engineers and programmers involved in invention and innovation.²¹⁸ Firms making substantial investments in R&D may engage in greater delegation of authority and provide more stock options as incentives for non-executive employees.²¹⁹ Companies are also significantly increasing the use of long-term incentive contracts for managers of R&D units.²²⁰

The problem of rewarding exploratory performance is related to the issue of rewarding agents when the contract cannot be based on the principal's objective. Difficulties in measuring performance limit

214. See Roger B. Myerson, *Perspectives on Mechanism Design in Economic Theory*, 98 AM. ECON. REV. 586, 587 (2008) ("[I]ncentive constraints express the basic fact that individuals will not share private information or exert hidden efforts without appropriate incentives.").

215. See PATRICK BOLTON & MATHIAS DEWATRIPONT, *CONTRACT THEORY* 95–96 (2005); JEAN-JACQUES LAFFONT & DAVID MARTIMORT, *THE THEORY OF INCENTIVES* 29 (2002); Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305, 308 (1976).

216. Poblete & Spulber, *supra* note 39, at 54.

217. *Id.* at 38.

218. Fredrik Andersson et al., *Reaching for the Stars: Who Pays for Talent in Innovative Industries?*, 119 ECON. J. F308, F327 (2009) ("We show that software firms that operate in software sectors with highly skewed returns to innovation, or high upside gains to innovation, are more likely to attract and pay for highly talented workers. Such firms do so first by paying more up-front in starting salaries to attract skilled employees and second by rewarding workers handsomely for experience or loyalty.").

219. John E. Core & Wayne R. Guay, *Stock Option Plans for Non-Executive Employees*, 61 J. FIN. ECON. 253, 272 (2001) ("Firms with greater monitoring costs and greater growth options (proxied by firm size, the book-to-market ratio, and R&D expense) provide greater option incentives to non-executive employees.").

220. Josh Lerner & Julie Wulf, *Innovation and Incentives: Evidence from Corporate R&D*, 89 REV. ECON. STAT. 634, 634 (2007) ("Among firms with a centralized R&D organization, a clear relationship emerges: more long-term incentives granted to corporate R&D heads are associated with more heavily cited patents. These incentives also appear to be associated with more frequent awards and patents of greater originality.").

reliance on monitoring employees.²²¹ However, “high-powered” incentives directly tied to individual performance are often problematic. For example, rewarding R&D personnel based on the number of patents may generate lower quality patents than rewards based on overall performance of the firm.²²² Even if the profit or stock price of the firm is observable, it can be difficult to anticipate the relationship between the benefits to the firm and the outcome of invention, innovation, or technology adoption.

Measuring performance may be problematic when basic inventions must undergo extensive development. This can generate delays in realizing the benefits of scientific and technological discoveries. Basic inventions often do not generate market returns without commercialization.²²³ Obtaining rewards from inventions generally requires application in innovative products, production processes, and transaction methods.²²⁴

Another important aspect of ICs is that specialized research personnel engaged in exploratory performance may respond well to intrinsic motivation.²²⁵ When R&D employees respond to intrinsic motivation, they may have an increased willingness to take risks.²²⁶ Risk taking may be desirable in R&D because employees may pursue projects involving greater creativity and may devote more effort to experimentation.²²⁷ Companies can design contracts and rewards that emphasize intrinsic motivation.

Kevin Murdock argues that the pharmaceutical company Merck’s Mectizan Donation Program illustrates contracting with intrinsic motivation.²²⁸ Merck developed the drug Mectizan as a cure for river blindness and offered the drug to potential users for free.²²⁹ The Mectizan Donation Program states that it is “the longest-running drug donation program for Neglected Tropical Diseases,” with over 300 million

221. Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization*, 62 AM. ECON. REV. 777, 780 (1972).

222. See George P. Baker, *Incentive Contracts and Performance Measurement*, 100 J. POL. ECON. 598, 609 (1992).

223. David M. Anderson, *Commercialization, HALF COST PRODUCTS*, <http://www.halfcostproducts.com/commercialization.htm> (last visited Nov. 9, 2018).

224. *Id.*

225. Todd Dewett, *Linking Intrinsic Motivation, Risk Taking, and Employee Creativity in an R&D Environment*, 37 R&D MGMT. 197, 197 (2007).

226. See *id.*; see also Markus Baer et al., *Rewarding Creativity: When Does it Really Matter?*, 14 LEADERSHIP Q. 569, 571 (2003).

227. Dewett, *supra* note 225, at 204.

228. Kevin Murdock, *Intrinsic Motivation and Optimal Incentive Contracts*, 33 RAND J. ECON. 650, 653 (2002).

229. *Id.*

treatments per year for river blindness (onchocerciasis) and lymphatic filariasis elimination.²³⁰ According to Murdock, a firm and its research personnel derive gains from trade when employees have intrinsic motivation.²³¹ Although the Mectizan project had negative financial returns for Merck, the firm benefitted because its research employees worked harder on other projects.²³² With intrinsic motivation, a firm realizes benefits from joint enforcement of multiple implicit contracts.²³³

Richard Gruner argues that patents encourage inventors to “dream big” and complete their projects.²³⁴ He identifies some psychological aspects of invention and innovation that can generate errors:

At least four psychological factors make it difficult for inventors to produce successful inventions based on distinctively new designs. These include: 1) difficulties in projecting the capabilities of new technologies in ways that point to new and distinctively different product designs; 2) divergences in the knowledge and experience of product inventors and product users, causing inventors to imperfectly understanding the functional needs and problems of potential invention users; 3) gaps in knowledge and experience of product inventors concerning the contexts where new inventions will be produced, supplied, and used, and; 4) inabilities of inventors to fully imagine the impacts of new inventions in use and the relative happiness of users with new inventions compared with alternative means for producing similar practical results.²³⁵

Gruner suggests changes in patent laws that would provide incentives for inventors that overcome these psychological problems.²³⁶ However, it is unlikely that patent law can be fine-tuned to address problems of inventor imagination.

In contrast, private ordering through contract terms can avoid the problems of a one-size-fits-all system of government grants. Patent

230. Overview, MECTIZAN DONATION PROGRAM, <https://mectizan.org/what/overview/> (last visited Nov. 11, 2018).

231. Murdock, *supra* note 228, at 651.

232. *Id.* at 667 (“When workers are intrinsically motivated, there are ‘gains from trade’ that arise when the firm implements a project that has negative financial return but generates large intrinsic returns to the agent.”).

233. *Id.*

234. Richard S. Gruner, *Imagination, Invention, and Patent Incentives: The Psychology of Patent Law*, 2017 U. ILL. J.L. TECH. & POL’Y 375, 435 (2017).

235. *Id.* at 380.

236. *Id.* at 382.

examination rules are legal standards applied by patent examiners.²³⁷ In contrast to these legal rules, firms can be flexible and adaptable. Firms can adjust contract terms depending on the industry, the product, the type of technology, and even the capabilities of individual researchers. Firms can also vary contract terms over time in response to changes in competition, scientific discoveries, regulation, and consumer demand.

Through the use of ICs, firms are able to design contracts that improve incentives for exploratory performance for employees, managers, and subcontractors. Firms can induce exploratory performance by offering basic rewards contingent on the overall financial performance of the firm. Firms can coordinate invention, commercialization, and innovation to provide rewards for exploratory performance. Firms can offer a combination of extrinsic rewards and intrinsic motivation to help induce creative performance. Firms can design ICs that help inventors overcome psychological barriers to creativity.

E. ICs and Fundamental Uncertainty

Technological change involves fundamental uncertainty that may not be present in most standard contracts.²³⁸ ICs provide basic mechanisms such as royalties and options that address fundamental uncertainty.²³⁹ Even when parties to a contract face risk with a known likelihood of events, it is difficult and costly to form contingent contracts.²⁴⁰ With fundamental uncertainty, contingent contracting becomes more difficult—to the point that any IC will likely be incomplete. Contract law tends to limit contractual constraints on renegotiation and therefore favors simpler contract forms.²⁴¹

Parties forming ICs encounter various forms of fundamental uncertainty that I refer to as statistical, discovery, creativity, and market uncertainty. Statistical uncertainty describes researchers' uncertainty about the outcome of their experiments. Researchers typically design experiments and gather the data generated by those experiments. Researchers usually do not know the characteristics of the population

237. See Stuart J.H. Graham et al., *The USPTO Patent Examination Research Dataset: A Window on Patent Processing*, 27 J. ECON. & MGMT. STRATEGY 554, 557 (2018).

238. See generally DAVID C. MOWERY & NATHAN ROSENBERG, *TECHNOLOGY AND THE PURSUIT OF ECONOMIC GROWTH* (1989). I do not consider various types of legal uncertainty that may affect ICs. These include uncertainty about approval of a patent application and whether a patent will be found to be valid and infringed in court proceedings.

239. See Poblete & Spulber, *supra* note 39, at 54.

240. See Ronald A. Dye, *Costly Contract Contingencies*, 26 INT'L ECON. REV. 233, 233–34 (1985).

241. Schwartz & Watson, *supra* note 38, at 26; see Poblete & Spulber, *supra* note 39 (discussing of renegotiation possibility effects on the form of incentive contracts).

from which the data was drawn, which is typically expressed as the lack of knowledge about the form of the probability distribution regarding some features of the population.²⁴² Researchers may not know anything about the form of the distribution, or researchers may know something about the form of the distribution but not specific parameter values of the distribution. This lack of knowledge can affect researchers' decisions in many different ways.²⁴³

Researchers use statistical inference to characterize the probability distribution that generates the data.²⁴⁴ Given samples drawn from an unknown population distribution, researchers make inferences about what is the form of the distribution.²⁴⁵ Statistical inference may take the form of estimation, construction of intervals that reflect a particular level of confidence, and hypothesis testing.²⁴⁶

Even if researchers learn something about the population distribution, they still may not know the distribution with certainty.²⁴⁷ Thus, the process of experimentation and statistical inference does not fully eliminate uncertainty. The uncertainty can be described using probability, but even these probabilities may not be known with accuracy.²⁴⁸

Discovery uncertainty refers to lack of knowledge about the future discoveries of other researchers. This reflects not only uncertainty about the outcome of particular experiments but also uncertainty regarding the types of experiments undertaken by other researchers and professional interactions among researchers. Researchers benefit from the past discoveries of others. As Isaac Newton wrote, "If I have seen further, it

242. See LARRY WASSERMAN, *ALL OF STATISTICS: A CONCISE COURSE IN STATISTICAL INFERENCE* 87 (2013), http://static.stevereads.com/papers_to_read/all_of_statistics.pdf.

243. See Martin Weber & Colin Camerer, *Recent Developments in Modelling Preferences Under Risk*, 9 OPERATIONS-RESEARCH-SPEKTRUM 129 (1987); see generally Colin Camerer & Martin Weber, *Recent Developments in Modeling Preferences: Uncertainty and Ambiguity*, 5 J. OF RISK & UNCERTAINTY 325 (1992) (providing examples of useful surveys).

244. See WASSERMAN, *supra* note 242, at 5.

245. *Id.* at 90.

246. *Id.*

247. See David Dequech, *Fundamental Uncertainty and Ambiguity*, 26 E. ECON. J. 41, 50–51 (2000) ("Going beyond situations of ambiguity, members of different schools of heterodox economic thought have emphasized situations of uncertainty of a more radical type. These situations are essentially characterized by the possibility of creativity and structural change and therefore by significant indeterminacy of the future. Uncertainty appears here in a dynamic context, in which the passage of time is crucial. The future cannot be anticipated by a fully reliable probabilistic estimate because *the future is yet to be created.*").

248. *Id.*; see generally JOHN MAYNARD KEYNES, *TREATISE ON PROBABILITY* (1921), <https://archive.org/stream/treatiseonprobab007528mbp#page/n105/mode/2up/search/uncertainty>.

is by standing on the shoulders of giants.”²⁴⁹ However, new discoveries will support or refute past discoveries. This effect compounds the statistical uncertainty researchers face when carrying out a particular project because the outcome of many other projects will impact the value of their work.

Science proceeds through discoveries that may confirm, extend, or refute previous discoveries. Thomas Kuhn argues that the development of scientific knowledge depends on a series of contentious revolutions.²⁵⁰ Each area of scientific inquiry goes through phases associated with dominant conceptual paradigms during which “normal-scientific research is directed to the articulation of those phenomena and theories that the paradigm already supplies.”²⁵¹ As Kuhn observes:

Discovery commences with the awareness of anomaly, i.e., with the recognition that nature has somehow violated the paradigm-induced expectations that govern normal science. It then continues with a more or less extended exploration of the area of anomaly. And it closes only when the paradigm theory has been adjusted so that the anomalous has become the expected.²⁵²

Israel Scheffler questions the revolution metaphor, emphasizing instead the scientific evaluation of evidence: “The *quality* of scientific deliberations makes for a special and rare form of argumentation. It demands responsibility to the evidence, openness to argument, commitment to publication, loyalty to logic, and an admission, in principle, that one may turn out to be wrong.”²⁵³

Whether through contentious revolutions or reasoned debate, new scientific discoveries cause researchers to reevaluate past discoveries. It is not feasible for ICs to address such complex contingencies. ICs for delegated or cooperative research are necessarily incomplete. IC design and legal rules thus need to provide general incentives for performance under discovery uncertainty.

249. Letter from Isaac Newton to Robert Hooke (Feb. 5, 1675) (on file with the Historical Society of Pennsylvania Digital Library), <https://digitallibrary.hsp.org/index.php/Detail/objects/9792>.

250. THOMAS S. KUHN, *THE STRUCTURE OF SCIENTIFIC REVOLUTIONS* 2 (2d enlarged ed., 1970).

251. *Id.* at 24.

252. *Id.* at 52–53.

253. Israel Scheffler, *Vision and Revolution: A Postscript on Kuhn*, 39 *PHIL. SCI.* 366, 374 (1972).

Creativity uncertainty refers to the lack of knowledge about what other inventors and innovators will develop. It is difficult, if not impossible, to predict the outcomes of invention and innovation.²⁵⁴ The limitless variety of creativity that is evident in the arts, such as music or literature, extends to invention and innovation in commerce, science, and technology. The creations of inventors and innovators inspire future creativity, further complicating uncertainty.

The creativity of inventors and innovators affects the economic value of past inventions and innovations. Inventions and innovations generate technological change that can enhance or diminish the past contributions of inventors, innovators, and adopters. Just as with discovery uncertainty, it is difficult, if not impossible, for an IC to address contingencies based on the creativity of other inventors and innovators. IC rules must therefore address the complexities of inventor and innovator creativity.

The creativity of other economic actors affects the expectation interests of parties to an IC in unpredictable ways. Advances in technology can serve as complements for existing technology and improve the performance of existing inventions and innovations. For example, advances in software can improve the demand for computer hardware.²⁵⁵ Conversely, advances in technology can be substitutes for existing technology, leading to its obsolescence. For example, smart phones have displaced basic mobile phones. This corresponds to Joseph Schumpeter's concept of "creative destruction."²⁵⁶

The novel and non-obvious criteria for the patentability of an invention illustrate creativity uncertainty.²⁵⁷ Novelty and non-obviousness are fleeting. An invention is a new and useful production process, machine, manufacturing technique, or composition of matter.²⁵⁸ Patents are granted for novel inventions, but novelty is not a guarantee of market value because new technologies can readily supersede a patent long before it expires.²⁵⁹ Obviousness is also subject to fundamental uncertainty. Based on experiments, Gregory Mandel observes:

254. David Dequech, *Expectations and Confidence Under Uncertainty*, 21 J. POST KEYNESIAN ECON. 415, 416 (1999).

255. EUROPEAN PATENT OFFICE & HANDELSBLATT RESEARCH INST., PATENTS AND THE FOURTH INDUSTRIAL REVOLUTION: THE INVENTIONS BEHIND DIGITAL TRANSFORMATION 20 (2017), [https://documents.epo.org/projects/babylon/eponet.nsf/0/17FDB5538E87B4B9C12581EF0045762F/\\$File/fourth_industrial_revolution_2017__en.pdf](https://documents.epo.org/projects/babylon/eponet.nsf/0/17FDB5538E87B4B9C12581EF0045762F/$File/fourth_industrial_revolution_2017__en.pdf).

256. JOSEPH SCHUMPETER, CAPITALISM, SOCIALISM, AND DEMOCRACY 83 (Routledge 2006) (1942).

257. 25 U.S.C. §§ 102–03 (2018).

258. 35 U.S.C. § 101 (2018).

259. Suzanne Scotchmer & Jerry Green, *Novelty and Disclosure in Patent Law*, 21 RAND J. ECON. 131, 146 (1990).

The results are dramatic: the hindsight bias prejudices patent decisions far more than anticipated. Not only are patent decisions routinely and unintentionally made in contradiction to patent doctrine, but even more significantly, patent law itself is incoherent. Judges, jurors, and patent examiners seemingly lack the cognitive ability to make decisions in the manner that patent law currently requires.²⁶⁰

Private agreements fill in many of the gaps left by public awards of IP and judicial decisions on patent validity. IC rules and the design of agreements can address the creativity effects of technological change. ICs reflect the parties' expectations and respond to their perceptions of what is new or obvious. The parties to an IC are better placed to evaluate how the creativity of others will affect their economic benefits. ICs handle much of what happens after the grant of IP.

Market uncertainty refers to unknown demand and costs, which can be heightened by the effects of technological change. We do not know what the demand for inventions will be in advance, particularly when the inventions have not been fully developed or tested. It is difficult, if not impossible, to predict the demand for innovations because they are new to the market. Some innovations, such as smart phones, diffuse rapidly and change the economy, and yet other innovations may be unsuccessful. It is also difficult for companies to estimate how adopting innovations will affect their costs and revenues. Additionally, companies face difficulties predicting competitor innovations and the effects that those innovations will have on market outcomes.

Market uncertainty represents fundamental uncertainty. It is difficult to determine market demand and supply because knowledge about demand and costs is dispersed among individual consumers and firms. Friedrich Hayek observes that society's economic problem is "the utilization of knowledge not given to anyone in its totality."²⁶¹ Hayek emphasizes that "the sort of knowledge with which I have been concerned is knowledge of the kind which by its nature cannot enter into statistics and therefore cannot be conveyed to any central authority in statistical form."²⁶² For Hayek, prices help to coordinate transactions by making the best use of dispersed knowledge.²⁶³ The price system is essential as an

260. Gregory N. Mandel, *Patently Non-Obvious: Empirical Demonstration that the Hindsight Bias Renders Patent Decisions Irrational*, 67 OHIO ST. L.J. 1391, 1393 (2006).

261. F. A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 520 (1945).

262. *Id.* at 524.

263. *Id.* at 526.

adjustment mechanism: “It is, perhaps, worth stressing that economic problems arise always and only in consequence of change.”²⁶⁴

Hayek argues that market uncertainty presents even greater difficulties than scientific uncertainty.²⁶⁵ This is because market outcomes are fleeting and lack the relatively greater stability of scientific discoveries:

The difference between economic competition and the successful procedure of science is that the former exhibits a method of discovering particular temporary circumstances, while science seeks to discover something often known as “general facts,” i.e., regularities in events, and is concerned with unique, particular facts only to the extent that they tend to refute or confirm its theories.²⁶⁶

Because of market uncertainty, Hayek observes that “competition is important primarily as a discovery procedure whereby entrepreneurs constantly search for unexploited opportunities that can also be taken advantage of by others.”²⁶⁷

The need to coordinate transactions becomes even more important when dealing with invention, innovation, and adoption. Market uncertainty has greater effects with technological change because inventions and innovations are untested. This makes ICs the essential means of addressing dispersed knowledge and adjusting to technological change.

III. INTELLECTUAL CONTRACT TYPES

ICs protect the expectation interests of parties involved in technological change, including inventors, innovators, and adopters. This section considers various types of IC, including employment contracts, outsourcing contracts, licensing contracts, research joint ventures, and intermediary and collective rights organizations.

A. *Employment Contracts*

Companies hire specialized personnel to carry out invention, innovation, and adoption. Employment contracts between firms and specialized personnel are an important form of IC. Firms use ICs with

264. *Id.* at 523.

265. *Id.* at 523–24.

266. F. A. Hayek, *Competition as a Discovery Procedure*, 5 Q. J. AUSTRIAN ECON. 9, 11 (Marcellus S. Snow trans., 2002) (1968).

267. *Id.* at 18.

managers and employees to create new products, production processes, transaction methods, and organizations.²⁶⁸

Most R&D is a delegated activity. R&D refers to basic research, applied research, and experimental development.²⁶⁹ R&D is the process of discovery and knowledge creation. Designing employment contracts for delegated R&D can be challenging because R&D generates both explicit and tacit knowledge. Tacit knowledge can be difficult and costly to observe, transfer, and reproduce.²⁷⁰

Annual expenditures on R&D in the US exceed one-half trillion dollars.²⁷¹ Industry provides the main source of this funding (\$347.7 billion); the other sources are the federal, state, and local governments (\$140.2 billion), academia (\$19.3 billion), and non-profits (\$20.3 billion).²⁷² R&D is performed primarily by industry (\$366.8 billion), with other R&D being carried out by academia (\$75.2 billion), government agencies (\$62.7 billion), and non-profits (\$22.8 billion).²⁷³

Just as firms have production functions for goods and services, firms also have production functions for knowledge.²⁷⁴ The knowledge production function describes how a firm uses R&D investment and employment to create intangible assets. The knowledge production function applies to creation of knowledge by a single firm or by groups of firms.²⁷⁵ Firms produce intangible assets including various types of IP: patents, trademarks, copyrights, and trade secrets. Intangible assets also

268. ORG. FOR ECON. COOPERATION AND DEV. & STATISTICAL OFFICE OF THE EUROPEAN CMTYS., OSLO MANUAL: GUIDELINES FOR COLLECTING AND INTERPRETING INNOVATION DATA 16–17 (3d ed. 2005) (“The Manual defines four types of innovations that encompass a wide range of changes in firms’ activities: product innovations, process innovations, organisational innovations and marketing innovations.”); see generally Stephen Bryan et al., *CEO Stock-Based Compensation: An Empirical Analysis of Incentive-Intensity, Relative Mix, and Economic Determinants*, 73 J. BUS. 661 (2000) (discussing contracts with executives).

269. ORG. FOR ECON. COOPERATION AND DEV., FRASCATI MANUAL 2015: GUIDELINES FOR COLLECTING AND REPORTING DATA ON RESEARCH AND EXPERIMENTAL DEVELOPMENT 45 (2015), <https://www.oecd-ilibrary.org/docserver/9789264239012-en.pdf?expires=1541275882&id=id&accname=guest&checksum=C5F78E17C5D5D32FCCC469D632ACF256> (“The term R&D covers three types of activity: basic research, applied research and experimental development.”).

270. *Id.* at 28 (“For an activity to be an R&D activity, it must satisfy five core criteria. The activity must be: novel, creative, uncertain, systematic, transferable and/or reproducible.”).

271. See 2017 *Global R&D Funding Forecast*, R&D MAG., Winter 2017, at 7, https://edisciplinas.usp.br/pluginfile.php/3378934/mod_resource/content/1/RD%202016.pdf (“For 2017, total U.S. R&D spending is expected to increase by 2.9% to \$527.5 billion or a 1% increase after accounting for 2017’s expected 1.9% inflation rate (EIU/OECD).”).

272. *Id.*

273. *Id.*

274. See Zvi Griliches, *Issues in Assessing the Contribution of Research and Development to Productivity Growth*, 10 BELL J. ECON. 92, 94–95 (1979).

275. *Id.*; see also Adam B. Jaffe, *Technological Opportunity and Spillovers of R&D: Evidence from Firms’ Patents, Profits and Market Value*, 76 AM. ECON. REV. 984, 989 (1986).

include reports of research results, statistical studies, scientific journal articles, software, blueprints, and invention prototypes. Firms produce inventions by employing researchers who have particular skill, judgment, motivation, creativity, and education. Firms invest in laboratory facilities and equipment. A firm may also apply a stock of intangible assets and licensing to produce intangible assets.

Employment contracts protect the interests of managers and employees who devote effort to R&D. Employment contracts must provide incentives for researchers to devote efficient effort to R&D, to make efficient decisions, and to report information accurately.²⁷⁶ Also, ICs for invention must address who owns the resulting inventions if R&D is successful.

Employment contracts also protect the expectation interests of employers. Firms provide wages and salaries, employee benefits, and training; invest in intangible assets, capital equipment, facilities, and complementary resources; and engage in procurement, marketing, sales, production, and distribution. Employment contracts must provide incentives for firms to hire specialized personnel and invest in technological change.

Companies commonly have significant numbers of employment contracts with research personnel. The Business R&D and Innovation Survey (BRDIS) estimates that there are about 1.5 million R&D workers in the U.S.;²⁷⁷ these employees include scientists, engineers, R&D managers, and support staff.²⁷⁸ Brandon Shackelford and Francisco Moris state:

Scientists and engineers are the researchers responsible for the design and creation of experiments, theories, and new products, processes, or methods. Technicians and other support staff typically work under the supervision of scientists and engineers and perform tasks such as computer programming, carrying out experiments, preparing statistical analysis, and clerical support and report writing.²⁷⁹

According to Donald Hecker:

High-technology occupations are scientific,

276. See Myerson, *supra* note 214.

277. Brandon Shackelford and Francisco Moris, NAT'L SCI. FOUND.: NAT'L CTR. FOR SCI. AND ENG'G STATISTICS, A SNAPSHOT OF BUSINESS R&D EMPLOYMENT IN THE UNITED STATES 1 (2016), <https://www.nsf.gov/statistics/2017/nsf17302/nsf17302.pdf>.

278. *Id.*

279. *Id.*

engineering, and technician occupations, the same group of occupations used to define high-tech industries in this and earlier studies. They include the following occupational groups and detailed occupations: computer and mathematical scientists, Standard Occupational Classification (soc) 15-0000; engineers, soc 17-2000; drafters, engineering, and mapping technicians, soc 17-3000; life scientists, soc 19-1000; physical scientists, soc 19-2000; life, physical, and social science technicians, soc 19-4000; computer and information systems managers, soc 11-3020; engineering managers, soc 11-9040; and natural sciences managers, soc 11-9120.²⁸⁰

The use of ICs for in-house R&D and outsourcing is not a new phenomenon. David Mowery examines industrial research between 1900 and 1940 and observes the growth of R&D both within manufacturing companies and in a network of independent research organizations.²⁸¹ Mowery finds that “[r]ather than functioning as substitutes, the independent and in-house research laboratories were complements during this period, exhibiting a division of labor in the performance of research tasks.”²⁸² Division of labor in the performance of research tasks among firms allows firms to specialize and gain greater expertise in particular areas of invention and innovation.²⁸³

Innovative firms must hire and motivate highly skilled managers and employees.²⁸⁴ Companies engaged in technological change offer specialized employee contracts and human resources management (HRM) policies.²⁸⁵ ICs for R&D managers and employees are likely to differ from other types of employment contracts. Pedro Ortín Ángel and Lluís Santamaria Sánchez argue that firms’ HRM practices must adapt to the particular needs of their R&D departments.²⁸⁶ They conduct case studies that examine various HRM practices in R&D, including the delegation of authority to specialized personnel, the provision of managerial support, the formation of multidisciplinary teams, internal

280. Daniel E. Hecker, *High-Technology Employment: A NAICS-Based Update*, MONTHLY LAB. REV. 57, 58 (2005).

281. David C. Mowery, *The Relationship Between Intrafirm and Contractual Forms of Industrial Research in American Manufacturing, 1900–1940*, 20 EXPLORATIONS IN ECON. HIST. 351 (1983).

282. *Id.* at 369.

283. *See id.* at 369–70.

284. Andersson et al., *supra* note 218, at F326.

285. Pedro Ortín Ángel & Lluís Santamaria Sánchez, *R&D Managers’ Adaptation of Firms’ HRM Practices*, 39 R&D MGMT. 271, 271 (2009).

286. *Id.*

and external networking opportunities, adjustment of recruitment policies, job rotation, career development, and compensation.²⁸⁷ Kathryn Martell and Stephen Carroll suggest firms' incentives for R&D personnel follow "promotion and pay policies that are congruent with employee expectations and company goals."²⁸⁸

Firms apply ICs to address the assignment of IP generated through the employment relationship. This represents a historical shift toward greater use of contracts.²⁸⁹ Catherine Fisk notes: "The law of employee inventions is an unstable mixture of the two bodies of law, the former honoring the rights of the *inventor* as employee, the latter being skeptical of the rights of the *employee* as inventor."²⁹⁰ From 1830 to 1930, Fisk recounts the change in law from an IP regime, in which the employee owns inventions, to a combination of employment contracts that assign inventions to the employer and state laws that include "shop rights" for employers.²⁹¹

Robert Merges examines the role of IP in employment contracts.²⁹² Merges observes that "[o]wnership is too blunt an instrument to be an effective inducement to employee-inventors."²⁹³ Based on economic analysis, Merges argues that "the law properly allows employers to take ownership of their employees' inventions."²⁹⁴ Employment contracts provide rewards for employees, specify employee duties, and allocate inventions:

[E]mployers have broad powers—consistently upheld by the courts—to claim employee inventions by contract. In addition, these contracts usually impose several related duties on employees, including (1) a duty to assign patent applications and patents to the employer, (2) a duty to assist in the patent prosecution, and (3) a general duty to

287. *Id.* at 284.

288. Kathryn D. Martell & Stephen J. Carroll Jr., *The Role of HRM in Supporting Innovation Strategies: Recommendations on How R&D Managers Should Be Treated from an HRM Perspective*, 25 R&D MGMT. 91, 92 (1995).

289. Catherine L. Fisk, *Removing the "Fuel of Interest" from the "Fire of Genius": Law and the Employee-Inventor, 1830-1930*, 65 U. CHI. L. REV. 1127, 1174 (1998).

290. *Id.* at 1128.

291. *Id.* at 1130–31 ("[M]ost employees who invent are bound by contracts requiring them to assign the patents to their employers.").

292. Robert P. Merges, *The Law and Economics of Employee Inventions*, 13 HARV. J.L. TECH. 1 (1999).

293. *Id.* at 37.

294. *Id.* at 3.

cooperate in the perfection of the employer's rights in the invention.²⁹⁵

Merges also considers three types of default rules under state law.²⁹⁶ First, when employees engage in "invention for hire," the firm owns the invention.²⁹⁷ Second, when non-R&D employees engage in firm-related invention, the employee may own the invention while the firm obtains a royalty-free license as a "shop right."²⁹⁸ Third, when employees engage in independent invention, they generally own the invention.²⁹⁹ Regarding employee exit, Merges concludes "both the default rules and the interpretation of post-employment contracts favor ex-employees."³⁰⁰

Employment contracts with specialized researchers are subject to asymmetric information. The firm may not be able to observe fully the employee's knowledge and skills. Also, it may be difficult for the firm to observe the experimental design and research activities of specialized employees. Then, ICs are subject to Principal-Agent problems in contract design.³⁰¹ Companies design ICs to provide performance incentives to specialized managers and employees engaged in invention and innovation.³⁰²

B. Outsourcing Contracts

Companies also use ICs to outsource invention and innovation to specialized research firms. Shackelford and Moris observe that the scientific R&D services industry is "dominated by contract research organizations that assist pharmaceutical, biotechnology, and medical device companies with clinical trials management."³⁰³ They find that the R&D services industry "employs relatively more technicians and support staff as a share of its domestic R&D employment than do most other industries."³⁰⁴ Firms contract with "star scientists" for access to knowledge and IP.³⁰⁵ In-house R&D is complementary to outsourcing

295. *Id.* at 8.

296. *Id.* at 5.

297. *Id.* at 5–6.

298. *Id.* at 6.

299. *Id.* at 6–7.

300. *Id.* at 47.

301. *Id.* at 26–27.

302. See Poblete & Spulber, *supra* note 39.

303. Shackelford & Moris, *supra* note 277, at 1.

304. *Id.*

305. Nicola Lacetera et al., *Do Firms Change Capabilities by Hiring New People? A Study of the Adoption of Science-Based Drug Discovery*, 21 *ADVANCES STRATEGIC MGMT.* 133 (2004); Lynne G. Zucker et al., *Commercializing Knowledge: University Science Knowledge Capture, and Firm Performance in Biotechnology*, 48 *MGMT. SCI.* 138 (2002).

R&D because internal knowledge helps the firm absorb external knowledge.

ICs that outsource R&D to a specialized research firm may face problems of moral hazard and adverse selection.³⁰⁶ The firm may compensate the specialized research firm based on some measure of invention or innovation, including revenues or profits.

Many companies outsource various invention and innovation activities.³⁰⁷ Paul Trott and Dap Hartmann find that “R&D departments have long recognised the importance of information and knowledge beyond their own organizations.”³⁰⁸ Companies rely on many types of strategic alliances, including “licensing, supplier relations, outsourcing, joint venture, collaboration (non-joint ventures), R&D consortia, industry clusters, and innovation networks.”³⁰⁹ Henry Chesbrough and others describe a trend toward increasing R&D cooperation among firms as “open innovation.”³¹⁰

It is estimated that companies obtain about half of their innovations from outside sources.³¹¹ Contracting to obtain R&D services from other firms is complementary to the firm’s internal R&D.³¹² For example, internal R&D increases a firm’s absorptive capacity for external knowledge.³¹³

306. Poblete & Spulber, *supra* note 39, at 39 (“Companies and government agencies also outsource R&D by contracting with research laboratories, specialized firms, universities, and independent researchers. . . . Corporations and venture capitalists also engage in delegation of R&D through financing, monitoring, and directing entrepreneurial technology startups, specialized research firms, and independent researchers.”).

307. Reinhilde Veugelers, *Internal R&D Expenditures and External Technology Sourcing*, 26 RES. POL’Y 303, 308 (1997); Peter Teirlinck et al., *Corporate Decision-Making in R&D Outsourcing and the Impact on Internal R&D Employment Intensity*, 19 INDUS. CORP. CHANGE 1741, 1742 (2010).

308. Paul Trott & Dap Hartmann, *Why ‘Open Innovation’ is Old Wine in New Bottles*, 13 INT’L J. INNOVATION MGMT. 715, 716 (2009).

309. *Id.* at 720.

310. Henry W. Chesbrough, *The Era of Open Innovation*, MIT SLOAN MGMT. REV., Spring 2003, at 35; Henry W. Chesbrough, *Why Companies Should Have Open Business Models*, MIT SLOAN MGMT. REV., Winter 2007, at 22.

311. Ashish Arora et al., *The Acquisition and Commercialization of Invention in American Manufacturing: Incidence and Impact*, 45 RES. POL’Y 1113, 1113 (2016) (“Our results indicate that, between 2007 and 2009, 16% of manufacturing firms had innovated—meaning had introduced a product that was new to the industry. Of these, 49% report that their most important new product had originated from an outside source, notably customers, suppliers and technology specialists (i.e., universities, independent inventors and R&D contractors).”).

312. Ashish Arora and Alfonso Gambardella, *The Market for Technology*, in 1 HANDBOOK OF THE ECONOMICS OF INNOVATION 641, 651 n.8 (Bronwyn H. Hall and Nathan Rosenberg eds., 2010).

313. Wesley M. Cohen and Daniel A. Levinthal, *Innovation and Learning: The Two Faces of R&D*, 99 ECON. J. 569, 589 (1989).

About four-fifths of world trade moves through a global supply chain involving networks of suppliers, distributors, and intermediaries.³¹⁴ The organization of production through global supply chains often involves contracts for outsourcing invention and innovation to supply chain managers and specialized research companies.³¹⁵ For example, pharmaceutical companies outsource clinical trials to Contract Research Organizations (CROs).³¹⁶

C. Joint Venture and Consortium Contracts

Firms use contracts to form RJVs and R&D consortia.³¹⁷ These are important types of IC. As with any joint venture, the RJV can take the form of a jointly-owned corporation, partnership, or contract without equity.³¹⁸ RJVs and consortia allow companies to cooperate in R&D while continuing to compete in product markets.³¹⁹ Joint ventures are an alternative to expansion of the firm through growth or mergers and acquisitions (M&A).³²⁰ Klaus Gugler and Ralph Siebert find that in the semi-conductor industry, RJVs tend to achieve greater efficiency gains than M&A.³²¹

Firms form R&D joint ventures and consortia to share the costs and risks of R&D.³²² By combining projects, the R&D joint venture can realize economies of scale in R&D, including specialization of function and division of labor for researchers. The firms may benefit from

314. See WORLD TRADE ORG., WORLD TRADE REPORT 2014: TRADE AND DEVELOPMENT: RECENT TRENDS AND THE ROLE OF THE WTO 43 (2014).

315. Jeremy Howells et al., *The Growth and Management of R&D Outsourcing: Evidence from UK Pharmaceuticals*, 38 R&D MGMT. 205, 206 (2008).

316. Pierre Azoulay, *Capturing Knowledge Within and Across Firm Boundaries: Evidence from Clinical Development*, 94 AM. ECON. REV. 1591, 1591 (2004).

317. For a discussion on JVs, see AM. BAR ASS'N, MODEL JOINT VENTURE AGREEMENT 359–72 (2006), <https://apps.americanbar.org/buslaw/newsletter/0049/materials/book.pdf>. For a discussion on R&D consortia, see Suzanne E. Majewski, *How Do Consortia Organize Collaborative R&D? Evidence from the National Cooperative Research Act* (Harvard Law Sch. John M. Olin Ctr. Law, Econ., Bus., Discussion Paper No. 483, 2004), <http://dx.doi.org/10.2139/ssrn.615583>.

318. AM. BAR ASS'N, *supra* note 317.

319. Majewski, *supra* note 317.

320. DELOITTE, A STUDY OF JOINT VENTURES THE CHALLENGING WORLD OF ALLIANCES 2 (2010), https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/finance/Publications/Etude_Joint_Venture_juillet%202010.pdf.

321. Klaus Gugler and Ralph Siebert, *Market Power Versus Efficiency Effects of Mergers and Research Joint Ventures: Evidence from the Semiconductor Industry*, 89 REV. ECON. STAT. 645, 651 (2007).

322. See James A. Dobkin, *Negotiating an International Technology Joint Venture*, 1 CONN. J. INT'L L. 81, 83 (1985); Joanna Poyago-Theotoky, *Equilibrium and Optimal Size of a Research Joint Venture in an Oligopoly with Spillovers*, 43 J. INDUS. ECON. 209, 209 (1995).

combining complementary skills and knowledge in R&D. Firms also may cooperate in R&D because it may be difficult to exclude access to each other's R&D. By combining R&D projects, the firms will appropriate the benefits of the knowledge created, thus internalizing potential spillovers that would result from separate projects.³²³ The RJV may also facilitate various business relationships, including agreements between suppliers and customers.³²⁴

The partners in an RJV may not be able to observe each other's R&D efforts or knowledge, which would lead to moral hazard and adverse selection problems. Addressing these problems requires dividing the benefits of the partnership based on some measure of performance. It may not be feasible to design an IC that induces sufficient R&D effort to maximize the joint benefits of the parties.³²⁵ Licensing arrangements affect the incentives of partners to share IP with the RJV.³²⁶

The National Cooperative Research Act (NCRA) of 1984 and the National Cooperative Research and Production Act (NCRPA) in 1993 limit antitrust liability for members of R&D consortia.³²⁷ These consortia report their membership to the Department of Justice (DOJ) and the

323. According to Yannis Caloghirou et al.:

Company incentives to join an RJV may include one or more of the following:

1. R&D cost sharing;
2. Reduction of R&D duplication;
3. Risk sharing, uncertainty reduction;
4. Spillover internalisation;
5. Continuity of R&D effort, access to finance;
6. Access of complementary resources and skills;
7. Research synergies;
8. Effective deployment of extant resources, further development of resource base;
9. Strategic flexibility, market access, and the creation of investment 'options';
10. Promotion of technical standards;
11. Market power, co-opting competition;
12. Legal and political advantages.

Yannis Caloghirou et al., *Research Joint Ventures*, 17 J. ECON. SURV. 541, 556 (2003).

324. Nicholas S. Vonortas, *Research Joint Ventures in the U.S.*, 26 RES. POL'Y 577, 591 (1997).

325. See Bengt Holmstrom, *Moral Hazard in Teams*, 13 BELL J. ECON. 324, 325 (1982); Karl Morasch, *Moral Hazard and Optimal Contract Form for R&D Cooperation*, 28 J. ECON. BEHAV. & ORG. 63, 65 (1995).

326. Sudipto Bhattacharya et al., *Licensing and the Sharing of Knowledge in Research Joint Ventures*, 56 J. ECON. THEORY 43, 44 (1992).

327. National Cooperative Research and Production Act of 1993, 15 U.S.C. §§ 4301–06 (2018); National Cooperative Research Act of 1984, 15 U.S.C. §§ 4301–05 (1984) (current version at 15 U.S.C. §§ 4301–06 (2018)).

Federal Trade Commission (FTC).³²⁸ From 1984 to 2008, 942 joint ventures registered with the antitrust agencies.³²⁹ The RJV may reduce competition between the partners but increase competition between the partners and other firms in the industry.³³⁰

Almost all joint ventures, even if they are not RJVs, involve parent companies licensing or transferring technology to the venture.³³¹ Kurt Saunders cautions that negotiation and planning of the RJV should address the disclosure, ownership, use, and management of IP contributed to or created by the venture.³³² The RJV agreement should also address the rights and duties of the partners and the joint venture regarding protection of IP, as well as infringement and misappropriation.³³³ RJVs can provide contractual protections for intangible assets when there are insufficient patent protections.³³⁴

D. License Contracts

ICs include IP license contracts. These types of contracts have a number of common features.³³⁵ The license contract describes the business relationship between the parties.³³⁶ The license contract specifies the period of time for the grant of rights to the licensee and lists the IP that is covered by the agreement.³³⁷ The contract may place various restrictions on the grant of rights.³³⁸ The Code of Federal Regulations states “the licensing of a patent transfers a bundle of rights which is less than the entire ownership interest, e.g., rights that may be limited as to time, geographical area, or field of use.”³³⁹ The licensing contract addresses IP issues that arise when either of the parties makes

328. Yves L. Doz et al., *Formation Processes of R&D Consortia: Which Path to Take? Where Does It Lead?*, 21 STRATEGIC MGMT. J. 239, 240 (2000).

329. See Majewski, *supra* note 317.

330. Janusz A. Ordover and Robert D. Willig, *Antitrust for High Technology Industries: Assessing Research Joint Ventures and Mergers*, 28 J. L. ECON. 311, 313–14 (1985).

331. Jordan, *supra* note 71, at 10.

332. Kurt M. Saunders, *The Role of Intellectual Property Rights in Negotiating and Planning a Research Joint Venture*, 7 MARQ. INTELL. PROP. L. REV. 75, 97 (2003).

333. *Id.* at 95.

334. Roberto Hernán et al., *An Empirical Evaluation of the Determinants of Research Joint Venture Formation*, 51 J. INDUS. ECON. 75, 87 (2003).

335. See DONALD M. CAMERON & ROWENA BORENSTEIN, KEY ASPECTS OF IP LICENSE AGREEMENTS 8 (2003), <http://www.jurisdiction.com/lic101.pdf>.

336. *Id.* at 7.

337. *Id.* at 32.

338. *Id.* at 12.

339. USPTO, MANUAL OF PATENT EXAMINING PROCEDURE (MPEP) § 301 (9th ed. 2015), <https://www.uspto.gov/web/offices/pac/mpep/s301.html#d0e17687>.

improvements to the technology.³⁴⁰ The contract also specifies the IP holder's compensation, including the way that royalties are calculated.³⁴¹

Most IP license contracts are specific to the business relationship between the licensor and the licensee.³⁴² This implies that most IP license contracts require bilateral negotiation that tailors the agreement to the needs of the relationship.³⁴³ License contracts offered by patent pools are an exception because they have standardized provisions and royalties.³⁴⁴

An IP license contract is designed to maximize the joint returns of the licensor and licensee.³⁴⁵ The most basic license gives the licensee access to the licensor's intangible assets.³⁴⁶ These licenses can serve to avoid litigation or resolve a dispute over IP.³⁴⁷ More complicated ICs involve additional business arrangements, including invention, innovation, investment, marketing, and complementary assets.³⁴⁸

License contracts may provide incentives for inventors to develop and transfer the invention and for adopters to apply the invention. The

340. CAMERON & BORENSTEIN, *supra* note 335, at 21 ("There is no widely accepted definition for 'improvement' in the context of intellectual property licenses, but it is usually used to mean a development within the field of the licensed technology that enhances the usability, functionality, efficiency, performance or other characteristic of the original technology.").

341. *See generally id.* (stating the contract also includes representations and warranties, disclaimers and limitations of liability, conflict resolution, contract termination and renewal, and enforceability).

342. Raymond C. Nordhaus, *Patent License Agreements*, 21 BUS. LAW. 643, 643 (1966) ("Because of the infinite variety of rights and obligations that may be established between a patent licensor and his licensee, there is no 'standard' form of license agreement that may be used in all situations. Each license agreement must be carefully tailored to the specific circumstances of the particular case."); Bharat N. Anand and Tarun Khanna, *The Structure of Licensing Contracts*, J. INDUS. ECON. 103, 131 (2000) ("Licensing contracts in the Computer and Electronics industries are more likely to be signed with firms with whom the licensor has prior relationships, established either through alliance activity, common board membership, or personnel histories.").

343. *See* Daniel F. Spulber, *Patent Licensing and Bargaining with Innovative Complements and Substitutes*, 70 RES. ECON. 693, 695 (2016).

344. *See id.* at 710.

345. *Id.* at 693.

346. Michael L. Katz and Carl Shapiro, *How to License Intangible Property*, 101 Q. J. ECON. 567, 568 (1986).

347. Sanford E. Warren Jr., *Intellectual Property Litigation Rising: How to Protect Your Company's Financial Health*, IRMI (Sept. 2009), <https://www.irmi.com/articles/expert-commentary/intellectual-property-litigation-rising-how-to-protect-your-company-s-financial-health>.

348. The demand for licenses is based on "carrots" if the user derives benefits from using the intangible asset. The demand for licenses is based on "sticks" if the user obtains the license to avoid litigation over disputed technology. Finally, the demand for licenses is based on "bundles" if the user obtains the license because it is included in a bundle with complementary goods and services. *See* Niklas Östman, *How to Create the 'Pull' for Patent Licensing?*, LINKEDIN (Sept. 6, 2016), <https://www.linkedin.com/pulse/how-create-pull-patent-licensing-niklas-%C3%B6stman?trk=prof-post>.

Principal-Agent problem involving hidden action or hidden information arises in licensing contracts.³⁴⁹ Richard Jensen and Marie Thursby study university licensing agreements and find most include both fixed fees and royalties; many also include sponsored research clauses and equity.³⁵⁰ The university licensing agreement with potential licensees involves a stage in which researchers continue to develop an invention.³⁵¹ This is a moral hazard problem because research efforts are not observable to the licensee. The licensing contract includes running royalties intended to induce inventor effort and lump-sum royalties that reflect potential earnings from commercialization of the invention.³⁵² Daniel Elfenbein considers university licensing agreements and observes the incidence of royalties based on sales, lump-sum license fees, milestones, maintenance fees and minimums, and equity.³⁵³

Inventors often have tacit knowledge that is complementary to their intangible assets. Inventors incur costs of codifying and communicating their knowledge to technology adopters.³⁵⁴ When it is very costly to transmit the inventor's knowledge, the inventor may have an advantage in applying that knowledge in comparison to technology adopters. Technology adopters may have advantages in applying the technology resulting from their own knowledge and complementary assets. This can overcome the problem of transmitting the inventor's tacit knowledge, resulting in technology transfers.³⁵⁵ Deepak Hegde explores how tacit knowledge affects the structure of royalties in licensing contracts, including royalty rates, lump-sum fees, milestones and minimum payments.³⁵⁶

349. See Inés Macho-Stadler et al., *The Role of Information in Licensing Contract Design*, 25 RES. POL'Y 43, 52 (1996) (discussing the role of information in determining the structure of royalties in patent licensing contracts); see also Nancy T. Gallini and Brian D. Wright, *Technology Transfer under Asymmetric Information*, 21 RAND J. ECON. 147 (1990).

350. Richard Jensen and Marie Thursby, *Proofs and Prototypes for Sale: The Licensing of University Inventions*, 91 AM. ECON. REV. 240 (2001).

351. *Id.* at 248.

352. See *id.* at 245.

353. Daniel W. Elfenbein, *Contract Structure and Performance of University-Industry Technology Transfer Agreements* (July 30, 2009), <https://ssrn.com/abstract=1452717>.

354. Daniel F. Spulber, *Tacit Knowledge with Innovative Entrepreneurship*, 30 INT'L J. INDUS. ORG. 641, 641 (2012).

355. *Id.*

356. Deepak Hegde, *Tacit Knowledge and the Structure of License Contracts: Evidence from the Biomedical Industry*, 23 J. ECON. MGMT. STRATEGY 568, 568 (2014).

E. Platform Contracts

Firms and cooperative organizations help establish and manage the market for innovative control.³⁵⁷ Firms and cooperative organizations use platform contracts to reduce transaction costs for both technology providers and technology adopters. Intermediary firms offer transaction efficiencies by market making, matching buyers and sellers, and reducing adverse selection and moral hazard.

Almost all markets are established by profit-maximizing firms acting as intermediaries.³⁵⁸ Firms provide intermediary services as market makers by purchasing and reselling goods and services.³⁵⁹ Such firms include retailers, wholesalers, and financial brokers.³⁶⁰ Market makers clear markets by balancing purchasing and sales and by posting and adjusting prices.³⁶¹ Firms also provide intermediary services by acting as matchmakers, bringing buyers and sellers together.³⁶² Market makers and matchmakers establish the rules of markets, referred to in finance as “market microstructure.”³⁶³ The Internet has given rise to platforms, which are digital market places. Intermediary firms that operate digital markets include Amazon, eBay, and Alibaba.

In the market for innovative control, just as in markets generally, there are intermediaries that improve the efficiency of transactions.³⁶⁴ By handling a high volume of transactions, intermediaries benefit from economies of scale and scope.³⁶⁵ These economies are due to benefits from sharing fixed costs across many units of output or across multiple products.³⁶⁶ Economies of scale and scope also result from specialization of function and division of labor among the employees of intermediary firms. A centralized intermediary can realize economies of scale and scope in the management of IP, keeping track of patent renewal fees, monitoring infringement, and defending patents against infringement. The centralized intermediary can provide convenience by licensing patent portfolios as bundles.

357. Daniel F. Spulber, *Market Microstructure and Intermediation*, 10 J. ECON. PERSP. 135, 141 (1996).

358. *Id.* at 135.

359. *Id.*

360. *Id.* at 137–38.

361. *Id.* at 136.

362. *Id.* at 145–46.

363. *Id.* at 135.

364. *Id.* at 146.

365. Spulber, *supra* note 77, at 293.

366. *Id.* at n.168.

Intermediary firms also improve transaction efficiencies by centralizing transactions.³⁶⁷ Buyers and sellers derive convenience from “one-stop-shopping.” A buyer can have access to the products of many sellers and a seller can reach many buyers, but any buyer or seller need only transact with the intermediary. In markets for innovative control, a licensee can obtain licenses for the technology of many licensors and a licensor can provide licenses to many sellers.

There are also transaction efficiencies from platforms that provide centralized contract negotiation.³⁶⁸ This is because buyers and sellers need only negotiate with the intermediary. This dramatically decreases the number of transaction relationships in comparison to the large number of bilateral transactions needed with decentralized contracting. With centralized contracting, agreements and compensation can be standardized. This allows licensors and licensees to have standardized contracts with the intermediary. This is particularly important in industries that have complex innovations requiring a combination of many different IP licenses.

IP intermediaries use ICs to address non-rivalrous consumption. The same technology can be used simultaneously by many firms to produce new inventions and to develop innovative products, production processes, and transaction methods. IP intermediaries provide central hubs to realize the returns from contracts with many adopters.

IP intermediaries address transaction costs in patent transfers and patent licensing.³⁶⁹ According to an FTC study of “Patent Assertion Entities,” about half of the companies in the study used patent acquisition contracts that shared licensing revenue with the inventor or employer of the inventor.³⁷⁰ The companies in the study acted as intermediaries between patent holders and licensees.³⁷¹

Some companies acquire patents and provide a “one-stop-shopping” platform for licensees. Consider for example, the patent intermediary Avanci:

367. Spulber, *supra* note 357, at 145.

368. Daniel F. Spulber, *The Economics of Markets and Platforms*, 28 J. ECON. MGMT. STRATEGY 159, 169–70 (2019).

369. Naomi R. Lamoreaux & Kenneth L. Sokoloff, *Intermediaries in the U.S. Market for Technology, 1870–1920* 28 (Nat’l Bureau of Econ. Research, Working Paper No. 9017, 2002), <https://www.nber.org/papers/w9017.pdf>; James F. McDonough III, *The Myth of the Patent Troll: An Alternative View of the Function of Patent Dealers in an Idea Economy*, 56 EMORY L.J. 189, 207 (2007).

370. FED. TRADE COMM’N, PATENT ASSERTION ENTITY ACTIVITY: AN FTC STUDY (2016), https://www.ftc.gov/system/files/documents/reports/patent-assertion-entity-activity-ftc-study/p131203_patent_assertion_entity_activity_an_ftc_study_0.pdf.

371. *Id.* at 100; see also John E. Dubiansky, *The Licensing Function of Patent Intermediaries*, 15 Duke L. & Tech. Rev. 269, 273 (2017).

Avanci has created the first platform for IoT manufacturers to license crucial, standard-essential wireless technologies with an emphasis on fair, transparent pricing. Avanci's pricing model offers flat rate royalty calculations that streamline licensing and enable predictable costs to help IoT developers capitalize on a dynamic market opportunity.³⁷²

Avanci emphasizes the benefits of "one-stop-shopping" and the implications of connectivity:

Products with wireless connectivity require access to thousands of patented inventions, created by many inventors. Avanci is bringing together standard-essential wireless patents that represent the most advanced wireless technology in the world, in an efficient, one-stop marketplace. So, instead of going to each technology owner to request, negotiate and pay for a license, makers of products for the Internet of Things can get the technology they need in one place.³⁷³

Avanci points out that transaction efficiencies increase incentives for innovation:

By providing licenses to essential wireless technology at fair rates, Avanci is helping ensure companies who need connectivity for their products can access it easily, and those creating wireless technology can share it as widely as possible. And both are incentivized to never stop innovating.³⁷⁴

IC intermediaries also include cooperative non-profit institutions such as patent pools and other Collective Rights Organizations (CROs).³⁷⁵ By offering transaction efficiencies, such private contracting institutions help to avoid antitrust scrutiny and government-mandated licensing.³⁷⁶

372. AVANCI, AVANCI: ACCELERATING IOT CONNECTIVITY 2 (2016), http://avanci.com/wp-content/uploads/2017/01/2016-Avanci-WP-Final-_-Jan-24.pdf.

373. *Technology*, AVANCI, <http://avanci.com/technology/> (last visited Jan. 21, 2019).

374. *Id.*

375. Robert P. Merges & Michael Mattioli, *Measuring the Costs and Benefits of Patent Pools*, 78 OHIO ST. L.J. 281, 285 (2017) ("The benefit for licensees is easy to appreciate: 'one stop shopping' for many patents at once. This conserves on the cost of licensing numerous patents from dispersed patent holders by, in a sense, compressing that process into a single event.").

376. Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CALIF. L. REV. 1293, 1295 (1996) ("Collective Rights Organizations (CROs) will often emerge to break the transactional bottleneck. From patent pools to collective copyright licensing organizations such as ASCAP and BMI, IPR owners in various industries have demonstrated the workability of these private transactional mechanisms. Indeed,

Robert Merges argues that “[t]he high costs of contracting—both among members, and between members and users—drive the right holders to pool their property rights in a collective organization.”³⁷⁷

Patent pools act as intermediaries and provide transaction platforms for patent holders and licensees.³⁷⁸ Patent pools reduce the transaction costs of combining licenses for complementary inventions.³⁷⁹ For example, MPEG LA, LLC provided a “one-stop-shopping” platform for licensing patents covering the international digital video compression standard MPEG-2.³⁸⁰ MPEG LA operated licensing programs covering “thousands of patents owned by hundreds of patent holders in nearly 100 countries with over 6,000 licensees.”³⁸¹

CONCLUSION

It has long been observed that “possession is nine-tenths of the law,” although there is much more to law than property. Similarly, discussions of knowledge and technological change tend to focus on IP. Yet, there is much more to Intellectual Law than IP.

The Intellectual Law framework introduced in this Article provides a comprehensive framework for dynamic efficiencies in technological change. The present discussion emphasizes that IC rules play an important role in Intellectual Law. ICs protect the expectation interests of those who invest in technological change. ICs allow variation in investment over time as parties make discoveries. IC law provides the basis for creating, developing, sharing, and applying intangible assets needed for technological change. IC rules enhance the economic contributions of both IP and IT rules.

IP provides the foundation of the market for innovative control, but IP is not sufficient for technological change. IP is incomplete and provides limited exclusivity. IP can be subject to public policy shocks that tend to weaken protections for inventors, innovators, and adopters. Also, the IT protections for inventors shift consent from IP owners to infringers. This suggests the need to reconsider the IP versus IT controversy in the context of contributions made by IC.

Technological change requires agreements that induce future performance. Cooperative investment generates invention, innovation, and technology adoption. Firms make these investments based on

these case studies uncover two distinct advantages of CROs: expert tailoring and reduced political economy problems.”).

377. *Id.* at 1302.

378. *Id.* at 1340–42.

379. *Id.* at 1340.

380. Lacy Horn, *Alternative Approaches to IP Management: One-stop Technology Platform Licensing*, 9 J. COM. BIOTECHNOLOGY 119, 120 (2003).

381. MPEGLA, <https://www.mpegla.com>. (last visited Feb. 16, 2019).

agreements with employees, suppliers, partners, investors, and customers. Technological change based on IC rules promotes economic development and drives economic growth.

ICs differ from standard contracts in various ways. ICs realize the benefits from non-rivalrous usage of technology through such mechanisms as licensing, cross-licensing, RJVs, R&D consortia, and one-stop-shopping platforms. ICs provide incentives for exploratory performance. ICs induce effort and revelation of information by rewarding performance using measures related to technological change. In contrast to contracts for the routine production of goods and services, ICs consider fundamental uncertainty. ICs must handle problems arising when contracting parties' efforts and information are unobservable and unverifiable. Such contracting difficulties are more likely to occur with invention and innovation than with more routine activities. ICs provide incentives for invention, innovation, and adoption. ICs achieve gains from trade in technology, thus increasing the rewards of IP holders beyond what they could achieve through IP alone.

The rate and direction of technological change have increased the shift toward IC. Greater connectivity and exchange of data among firms requires agreements for discovery and sharing knowledge. Increased emphasis of software over hardware means that inventions and innovations are virtual, further increasing the importance of intangible assets. The development of AI requires agreements between firms and employees and among firms to address new forms of knowledge creation. The technological development of the economy is transforming contracts and generating the need for a framework of "Intellectual Law."

THE CALIFORNIA CONSUMER PRIVACY ACT: TOWARDS A EUROPEAN-STYLE PRIVACY REGIME IN THE UNITED STATES?

*Stuart L. Pardau**

INTRODUCTION	69
I. PRIVACY LAW IN THE U.S.	73
A. <i>Modality-Focused Laws</i>	74
1. The TCPA	74
2. CAN-SPAM	75
3. The CFAA	76
4. Modality-Focused Laws in California	77
5. Other Modality-Focused Laws.....	78
B. <i>Content-Focused Laws</i>	79
1. The FCRA	79
2. IPAA	80
3. The GLBA.....	81
4. Content-Focused Laws in California	81
C. <i>Laws Protecting Children</i>	82
1. COPPA.....	82
2. California Laws Protecting Children	82
3. Other Laws Protecting Children.....	83
II. PRIVACY LAW IN EUROPE.....	83
A. <i>The EU Data Protection Directive</i>	84
B. <i>GDPR</i>	85
III. THE CALIFORNIA CONSUMER PRIVACY ACT	88
A. <i>The Ballot Initiative</i>	89
B. <i>The California Consumer Privacy Act</i>	91
1. Who (and What) Is Covered by the CCPA?	92
2. What Specific Rights Are Conferred on Consumers?	94
3. What Must Businesses Disclose in Their Privacy Policies?	98
4. What Additional Notifications Are Required?.....	98
5. What Remedies Do Consumers Have?	99
6. What Powers Does the Attorney General Have?	100

* J.D. Stanford Law School and Associate Professor, The David Nazarian College of Business and Economics, California State University, Northridge.

IV.	TOWARDS A EUROPEAN-STYLE PRIVACY REGIME?.....	100
A.	The CCPA, GDPR, and the Future of American Privacy Law	100
B.	Suggestions for Moving Forward.....	103
1.	Make the Private Right of Action More Meaningful	104
2.	Include a Whistleblower Provision	105
3.	Implement a More Effective Cure Period	106
4.	Clarify the Definition of “Publicly Available” Information.....	106
5.	Clarify the Deletion Requirement	107
6.	Clarify the Interplay with Federal Statutes	108
7.	Clarify the 12-Month Requirement.....	110
8.	Expand the Carve-Out for “Research”	110
9.	Streamline the Disclosure Requirements	112
	CONCLUSION.....	113

INTRODUCTION

When it comes to technology, over the last two decades the consuming public has rushed forward excitedly in all directions towards new and seemingly revolutionary services, without any deep thought about the business models of well-known tech giants or what important tradeoffs might be contained in the fine print of privacy policies or online terms and conditions.¹ Consumers value Facebook because it offers a way to stay connected with far-away friends, plus a place to raise online storefronts, organize events, and rally people to social or political causes.² Google can synchronize your email, contact list, calendar, and other core services, all while offering the most popular Internet search engine and

1. See, e.g., Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH: FACT TANK (Dec. 4, 2014), <http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>; Mark Sableman, *Who Reads Privacy Policies?*, THOMPSON COBURN LLP (May 31, 2017), <https://www.thompsoncoburn.com/insights/blogs/internet-law-twists-turns/post/2017-05-31/who-reads-privacy-policies/>; David Berreby, *Click to Agree with What? No One Reads Terms of Service, Studies Confirm*, GUARDIAN (Mar. 3, 2017, 8:38 AM), <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print>.

2. See, e.g., Kurt Wagner, *8 Ways Facebook Changed the World*, MASHABLE (Feb. 4, 2014), <https://mashable.com/2014/02/04/facebook-changed-the-world/#ziCS5YCLTaQV>; Jessica Elgot, *From Relationships to Revolutions: Seven Ways Facebook Has Changed the World*, GUARDIAN (Aug. 28, 2015), <https://www.theguardian.com/technology/2015/aug/28/from-relationships-to-revolutions-seven-ways-facebook-has-changed-the-world>.

what is now also the world's most popular browser.³ Instagram has perfected what Facebook's feed never quite got right: an elegant, uncluttered space for users to share snapshots of their lives.⁴

Alongside these platform-specific offerings, other new developments in the business of the Internet were also, as measured or gauged by the level of consumer adoption, accepted as obviously good—at least from a utilitarian perspective, the perceived benefit of these new services outweighed the perceived “detriments” associated with the sharing of one's personal information. To name two examples, geolocation services meant consumers could bring into harmony their physical locations with their “place” on the Internet,⁵ and the advent of targeted advertising meant more ads you wanted to see and fewer of those you did not.⁶

What could be the problem with any of this?

It has taken some time for consumers to apprehend and process a new reality: to see the Big Data forest for the individual platform trees, so to speak. If Web 1.0 was the Internet of free access to knowledge and a new,

3. *Browser & Platform Market Share: July 2018*, W3COUNTER, <https://www.w3counter.com/globalstats.php?year=2018&month=7> (last visited Feb. 17, 2019) (showing Chrome at 58% and Safari in a distant second at 14%); see Kris Holt, *15 Ways Google Changed the World*, DAILY DOT (Sept. 4, 2013), <https://www.dailydot.com/debug/google-15-anniversary-search-maps/>.

4. Eric Markowitz, *How Instagram Grew from Foursquare Knock-Off to \$1 Billion Photo Empire*, INC. (Apr. 10, 2012), <https://www.inc.com/eric-markowitz/life-and-times-of-instagram-the-complete-original-story.html>; Kim Mai-Cutler, *From 0 To \$1 Billion in Two Years: Instagram's Rose-Tinted Ride to Glory*, TECH CRUNCH (Apr. 9, 2012), <https://techcrunch.com/2012/04/09/instagram-story-facebook-acquisition/>.

5. See Chirag Kukarni, *15 Ways Geolocation Is Totally Changing Marketing*, FORTUNE (Feb. 6, 2017), <http://fortune.com/2017/02/06/geolocation-marketing/>; Janelle Nanos, *How Companies Use Geolocation Data to Target You*, BOS. GLOBE, <http://apps.bostonglobe.com/business/graphics/2018/07/foot-traffic/> (last visited Feb. 17, 2019) (“Geotargeted mobile marketing is one of the fastest growing forms of advertising—and one of the most controversial. . . . In 2017, marketers spent \$17.1 billion on geotargeted mobile ads, and the research firm BIA Advisory Services forecasts that number will more than double to \$38.7 billion by 2022.”). Despite recent widespread adoption of geolocation, there is evidence consumers were slower to adopt this particular technology, especially in the mobile context, than others. See, e.g., JVG, *Adoption of Geolocation Applications Is Still Stagnant*, VENTURE BEAT (Dec. 6, 2011, 11:13 AM), <https://venturebeat.com/2011/12/06/geosocial-app-adoption/> (“Thirty percent of online adults in the U.S. are familiar with geolocation applications, but less than six percent of online adults use these apps . . .”).

6. See Leslie K. John et al., *Ads That Don't Overstep*, HARV. BUS. REV., Jan.–Feb. 2018, at 62, <https://hbr.org/2018/01/ads-that-dont-overstep> (“The results [of targeted advertising] have been impressive. Research has shown that digital targeting meaningfully improves the response to advertisements and that ad performance declines when marketers' access to consumer data is reduced.”).

exhilarating, and vaguely utopian globalism, then it seems Web 2.0 is the “Internet of Things,” consumer profiling, predictive analytics, and targeted advertising.⁷ Following the 2018 Cambridge Analytica scandal, Facebook founder Mark Zuckerberg testified for nearly ten hours over the course of two days before both houses of Congress regarding Facebook’s privacy practices.⁸ These hearings were undoubtedly animated by the perception—real or imagined—that foreign powers had successfully meddled in the U.S. Presidential elections of 2016 through the medium of Facebook. Perhaps for the first time, the U.S. government seemed to be taking a real interest in Facebook’s essential business model and its implications for privacy, and even the nature of democracy. During the Senate hearing, Utah Senator Orrin Hatch asked Zuckerberg: “So, how do you sustain a business model in which users don’t pay for your service?” Zuckerberg replied, correctly: “Senator, we run ads.”⁹ So it seems that, even now, it is taking some time for public consciousness—and lawmakers—to catch up.

In contrast with American authorities, European authorities have been asking hard, existential questions about Internet privacy for decades, notably with regard to Facebook and Google: the two giants of Web 2.0.¹⁰ Most importantly, and as a kind of culmination of years of back and forth between the U.S. and Europe on these questions, the General Data Protection Regulation (GDPR) went into effect on May 25, 2018, implementing broad privacy protections for anyone “in the Union,” including non-citizens, and instituting remarkably hefty fines for violators.¹¹

Now, in the U.S. too, it seems there is budding awareness that Web 2.0 raises more far-reaching and extensive privacy concerns than the average user may have originally considered. It may be that, following this new awareness, and in an effort on the part of tech firms to get ahead of likely legal changes, the appetite for sweeping legislation in the U.S.

7. See Daniel Nations, *Is Web 3.0 Really a Thing?*, LIFEWIRE (Mar. 24, 2018), <https://www.lifewire.com/what-is-web-3-0-3486623> (discussing Web 1.0 and Web 2.0, and the possibility of a “Web 3.0” just around the corner).

8. See Cecilia Kang et al., *Mark Zuckerberg Testimony: Day 2 Brings Tougher Questioning*, N.Y. TIMES (Apr. 11, 2018), <https://www.nytimes.com/2018/04/11/us/politics/zuckerberg-facebook-cambridge-analytica.html>.

9. See Sean Burch, *‘Senator, We Run Ads’: Hatch Mocked for Basic Facebook Question to Zuckerberg*, S.F. CHRON. (Apr. 10, 2018), <https://www.sfchronicle.com/entertainment/the-wrap/article/Senator-We-Run-Ads-Hatch-Mocked-for-Basic-12822523.php>.

10. See, e.g., Suzanne Daley, *On Its Own, Europe Backs Web Privacy Fights*, N.Y. TIMES (Aug. 9, 2011), <https://www.nytimes.com/2011/08/10/world/europe/10spain.html>; Hannah Kuchler, *Max Schrems: The Man Who Took on Facebook—and Won*, FIN. TIMES (Apr. 5, 2018), <https://www.ft.com/content/86d1ce50-3799-11e8-8eee-e06bde01c544>.

11. See *infra* Part III.

is also on the rise.¹² Certainly, there are already a vast array of “privacy” laws on the books at both the state and the federal level. However, these have by and large been aimed at specific, ascertainably urgent and easier-to-understand problems such as data breach notification, protection of sensitive health and financial information, or children’s privacy.¹³ Following the Cambridge Analytica scandal, Zuckerberg’s testimony to Congress and the enactment of GDPR, it seems the Internet and digital privacy are having a moment. Now is a good time to ask whether sweeping legislation in the mold of GDPR might be around the corner in America.¹⁴

If so, it looks like California is already leading the way towards greater security of the consumer—or to needless overregulation, depending on one’s perspective.¹⁵ Governor Jerry Brown signed into law The California Consumer Privacy Act (CCPA or the Act) on June 28, 2018; it goes into effect on January 1, 2020.¹⁶

Broadly, the CCPA grants consumers four basic rights in connection to their personal data: (1) the right to know what personal information a business has collected about them and how it is being used; (2) the right to “opt out” of a business selling their personal information; (3) the right to have a business delete their personal information; and (4) the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.¹⁷ These rights are largely to be enforced by the California Attorney General, with a narrow private right

12. John D. McKinnon & Marc Vartabedian, *Tech Firms, Embattled Over Privacy, Warm to Federal Regulation*, WALL ST. J. (Aug. 6, 2018), <https://www.wsj.com/articles/tech-firms-embattled-over-privacy-warm-to-federal-regulation-1533547800> (“U.S. tech companies, battered over their handling of consumers’ personal data, are hoping to get ahead of the public and legal fallout by working with policy makers to help shape potential new federal privacy legislation.”).

13. See *infra* Part II.

14. See, e.g., Cameron F. Kerry, *Filling the Gaps in U.S. Data Privacy Laws*, BROOKINGS INST.: TECH TANK BLOG (July 12, 2018), <https://www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws/> (“The Cambridge Analytica stories, the Mark Zuckerberg hearings, and the constant reports of major data breaches have increased interest in federal privacy legislation. Various groupings have been convening to develop proposals. The time is ripe for interests to converge on comprehensive federal privacy legislation.”).

15. See Sarah Jeong, *No One’s Ready for GDPR*, VERGE (May 22, 2018, 3:28 PM), <https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu> (quoting PayPal founder Peter Thiel: “There are no successful tech companies in Europe and they are jealous of the US so they are punishing us.”).

16. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (2018) (effective Jan. 1, 2020).

17. Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER ROSE LLP: PRIVACY L. BLOG (July 13, 2018), <https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/> [hereinafter *Proskauer Summary*].

of action for data breaches.¹⁸ As discussed in more detail below, the bill was passed in response to—and to keep Californians from voting on—a ballot initiative presenting even more stringent privacy measures than what is contained in the CCPA.¹⁹ Although the bill will likely be amended before it goes into effect in 2020, the final law is almost certain to be a game changer for U.S. privacy.

Because it is the broadest, most overarching privacy law passed in the U.S. to date, the CCPA quickly drew comparisons to GDPR.²⁰ But is it, in fact, the first step towards a sea change in American privacy law towards a more “European” ethos? As this article explores, the answer to that question is “in some cases, yes, in others, no.” Irrespective of this narrow question, the passage of the CCPA presents an opportunity for deep reflection on privacy law in the U.S. and how best to move forward. Specifically, the purpose of this article is three-fold: (1) to briefly survey the privacy law status quo in the U.S. and Europe; (2) to provide an overview the CCPA; and (3) to offer some additional insights and recommendations on how best to further modify and enhance the CCPA to make it more effective in some areas and less sweeping in others. Parts II and III discuss privacy law in the U.S. and in Europe, respectively. Part IV discusses the CCPA, as it was presented in ballot initiative form, and as it was ultimately passed by the California legislature. Part V contemplates the CCPA’s potential effect on U.S. privacy law and makes some suggestions for how best to further modify and enhance the law. Part VI contains the conclusion.

I. PRIVACY LAW IN THE U.S.

In the absence of generalized privacy legislation like California’s CCPA, privacy law in the wider U.S. remains a complex patchwork of narrowly tailored federal and state laws. Aside from data breach notification laws,²¹ these privacy laws can generally be divided into three

18. See *infra* Section IV.B.

19. See *infra* Part IV.

20. See, e.g., Mike Khoury, *California’s Mini-GDPR? The Newly-Enacted California Consumer Privacy Act of 2018*, LEXOLOGY (July 10, 2018), <https://www.lexology.com/library/detail.aspx?g=60487525-76ea-44e3-97a8-3b9b02987c2e/>; Allison Grande, *Calif. Privacy Law to Spark GDPR-Like Compliance Efforts*, LAW360 (July 3, 2018, 10:13 PM), <https://www.law360.com/articles/1059877/calif-privacy-law-to-spark-gdpr-like-compliance-efforts>.

21. Data breach notification laws arguably constitute a fourth major category of privacy laws in the U.S. Although there is no generalized federal law governing security breaches, specific laws like GLBA and HIPAA include breach notification provisions. See *infra* Section II.B. More importantly, all fifty states and the District of Columbia now have their own data breach notification laws. Petrina McDaniel & Keshia Lipscomb, *Data Breach Laws on the Books in Every State: Federal Data Breach Law Hangs in the Balance*, SQUIRE PATTON BOGGS: SEC. & PRIVACY//BYTES (Apr. 30, 2018), <https://www.securityprivacybytes.com/2018/04/data->

categories: (1) laws focused on the modality used to collect or transmit personally identifiable information, such as telephone or email communications; (2) laws focused on the type of data collected and transmitted, or on a specific industry, such as health or financial information; and (3) laws aimed at protecting specific groups, such as children.²²

A. Modality-Focused Laws

On both the federal and state levels, a number of laws are aimed at protecting consumer privacy as it relates to a specific modality or method of communication. In every case, the legislation is designed to address what was originally a specific technological development or a set of exigencies which are unique to that particular modality, such as the proliferation of auto-dialers or email SPAM.

1. The TCPA

One of the most prominent among these modality-focused laws is the Telephone Consumer Protection Act (TCPA).²³ Enacted in 1991 in response to massive improvements in telephone dialing technology—and a resultant uptick in telemarketing—the TCPA was an effort by Congress to balance “[i]ndividuals’ privacy rights, public safety interests, and commercial freedoms of speech and trade.”²⁴

Broadly, the TCPA requires prior express consent before making any non-emergency calls using an “automatic telephone dialing system,” or “autodialer,” to three categories of phone lines: (1) any emergency line, including any “911” line; (2) “any guest room or patient room of a hospital, health care facility, elderly home, or similar establishment”; or (3) “any telephone number assigned to a . . . cellular telephone service.”²⁵ The statute provides that “[t]he term ‘automatic telephone dialing system’

breach-laws-on-the-books-in-every-state-federal-data-breach-law-hangs-in-the-balance/; see *Comparison of U.S. State and Federal Security Breach Notification Laws*, STEPTOE & JOHNSON (Jan. 21, 2016), <https://www.steptoel.com/images/content/6/5/v1/6571/SteptoelDataBreachNotificationChart.pdf>

22. See Luis Alberto Montezuma, *The Case for a Hybrid Model on Data Protection/Privacy*, IAPP (Feb. 27, 2018), <https://iapp.org/news/a/the-case-for-a-hybrid-model-on-data-protectionprivacy/> (describing the U.S. privacy regime as a “sectoral model” and the European approach as a “comprehensive model”).

23. 47 U.S.C. § 227 (2018). In addition to the statute itself, the broader universe of TCPA law also includes attendant regulations implemented by the Federal Communications Commission (FCC) and a number of rulings issued by the FCC which offer guidance on the law. *E.g.*, 47 C.F.R. § 64.1200 (2018).

24. Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991, 30 FCC Rcd. 7961, 7964, ¶ 2 (2015) [hereinafter FCC 2015 Order].

25. 47 U.S.C. § 227(b)(1)(A) (2018); 47 C.F.R. § 64.1200(a)(1) (2018).

means equipment which has the capacity²⁶—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers.”²⁷

In addition to authorizing state attorneys general and the FCC to enforce its rules,²⁸ the TCPA also has a private right of action provision, which mandates \$500 in statutory damages for each violation and up to \$1,500 for each willful violation with no cap on total damages;²⁹ the statute imposes a “strict liability” standard.³⁰ All of these factors together have made the TCPA an especially lucrative statute for the plaintiffs’ bar—and an especially enduring headache for businesses who regularly engage in telephone communications.³¹

2. CAN-SPAM

Just as the TCPA zeroed in on telephones, the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM) was the first law to set national standards for commercial email communications.³² CAN-SPAM covers all commercial messages, which are defined in the act as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service,” and makes no exception for business-to-business communications.³³

26. The autodialer definition, and specifically the FCC’s interpretation of the term “capacity,” has long been a source of controversy since a number of TCPA cases turn on whether the equipment used by a defendant was, in fact, an autodialer. In a 2015 ruling, the FCC concluded that the term “capacity” includes equipment’s “potential functionalities” or “future possibilit[ies],” not just its “present ability.” FCC 2015 Order at 7974 ¶ 16, 7975 ¶ 20. But on March 16, 2018, in a long-awaited opinion, the D.C. Circuit concluded that the Commission’s autodialer definition was arbitrary and capricious. *ACA Int’l v. FCC*, 885 F.3d 687, 699 (D.C. Cir. 2018) (“[T]he Commission’s interpretation of the term ‘capacity’ in the statutory definition of an ATDS is ‘utterly unreasonable in the breadth of its regulatory [in]clusion.’”).

27. 47 U.S.C. § 227(a)(1)(A)–(B). In addition to regulating telephone calls and text messages, the TCPA, as amended by the Junk Fax Protection Act (JFPA), also regulates telephone facsimile communications.

28. Richard P. Eckman, *The Telephone Consumer Protection Act Overview (Client Alert)*, PEPPER HAMILTON LLP (Nov. 23, 2015), <http://www.pepperlaw.com/publications/the-telephone-consumer-protection-act-overview-2015-11-23/>.

29. 47 U.S.C. § 227(b)(3).

30. See, e.g., *Alea London Ltd. v. Am. Home Servs., Inc.*, 638 F.3d 768, 776 (11th Cir. 2011) (“The TCPA is essentially a strict liability statute . . .”).

31. *Analysis: TCPA Litigation Skyrockets Since 2007; Almost Doubles Since 2013*, U.S. CHAMBER INST. FOR LEGAL REFORM (Feb. 5, 2016), <http://www.instituteforlegalreform.com/resource/analysis-tcpa-litigation-skyrockets-since-2007-almost-doubles-since-2013>.

32. 15 U.S.C. § 7701 (2018).

33. 15 U.S.C. § 7702(2)(A).

Generally, and as described by the Federal Trade Commission (FTC), CAN-SPAM has seven main requirements: (1) “[d]on’t use false or misleading header information;” (2) “[d]on’t use deceptive subject lines;” (3) “[i]dentify the message as an ad;” (4) “[t]ell recipients where you’re located;” (5) “[t]ell recipients how to opt out of receiving future emails from you;” (6) “[h]onor opt-out requests promptly;” and (7) “[m]onitor what others are doing on your behalf.”³⁴

Because it does not include a private right of action—only allowing the federal government, the attorney general of a state, and Internet service providers to bring actions—CAN-SPAM has not been the same kind of vehicle for litigation as the TCPA. But that does not mean that CAN-SPAM violations cannot be costly: the Act provides for civil and criminal penalties for noncompliance, including statutory damages up to \$6 million for willful violations, and even prison terms of up to five years.³⁵

3. The CFAA

Like the TCPA and CAN-SPAM, the Computer Fraud and Abuse Act (CFAA) was passed in 1984 to protect a specific type of equipment or “modality”—the computer systems of financial institutions and the federal government.³⁶ In 1994, the law was amended to include a private right of action; in 1996, the law was amended again to expand the definition of protected computers to encompass all computers used in foreign or interstate commerce.³⁷

The central prohibition of the CFAA applies to individuals who access protected computers “without authorization” or in a way that “exceeds authorized access.”³⁸ Under subsection (g) of the CFAA, “[a]ny person who suffers damage or loss by reason of a violation . . . may maintain a

34. *CAN-SPAM Act: A Compliance Guide for Business*, FED. TRADE COMM’N (Sept. 2009), <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>.

35. 15 U.S.C. § 7706(3)(C)(i)–(f)(1); *see also Technology Commentaries: The Federal CAN-SPAM Act—New Requirements for Commercial E-Mail*, JONES DAY (Feb. 2004), <http://www.jonesday.com/files/Publication/0ea34eeb-8735-41f6-ad24-5bdebf7a3433/Presentation/PublicationAttachment/26f5b006-e312-4e0e-8aa7-cab46b2126c3/Federal%20CAN-SPAM.pdf>.

36. 18 U.S.C. § 1030 (2018).

37. Lee Goldman, *Interpreting the Computer Fraud and Abuse Act*, 13 PITT. J. TECH. L. & POL’Y 1, 2 (2012) (“Whereas the Act originally applied to misuse of computers used by financial institutions or the United States government, the current version covers all computers used in or affecting commerce, including computers located outside the United States that affect commerce or communication in the United States. Given access to the Internet, this covers virtually all business, home and laptop computers.”).

38. 18 U.S.C. § 1030(a)(1).

civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.”³⁹ But private plaintiffs are limited to economic damages and must be able to show losses of at least \$5,000.⁴⁰

4. Modality-Focused Laws in California

Like a number of other states, California has its own laws aimed at protecting consumers’ privacy against invasive telemarketing practices. Most notably, Business and Professions Code Sections 17590–17594 enshrine a state “do not call” list based on the national “do not call” list;⁴¹ Public Utilities Code Sections 2871–2876 requires robocalls to be introduced by a live person;⁴² and the Business and Professions Code Section 17538.41 prohibits unsolicited text advertisements to cell phones or pagers.⁴³

Aside from telephone communications, Business and Professions Code Sections 17529 and 17538.45, like CAN-SPAM, also regulate unsolicited commercial email.⁴⁴ Mirroring the CFAA, Penal Code Section 502 likewise imposes criminal sanctions for accessing, and without permission, using, abusing, damaging, contaminating, disrupting, or destroying a computer system or network.⁴⁵ And perhaps more so than any other state, California also has a host of privacy laws registering more specific modalities, which range from automated license

39. 18 U.S.C. § 1030(g).

40. Goldman, *supra* note 37, at 3.

41. CAL. BUS. & PROF. CODE §§ 17590–17594 (West 2018) (“Thus, it is the intent of the Legislature to adopt the California telephone numbers on the national ‘do not call’ registry as the California ‘do not call’ registry.”).

42. CAL. PUB. UTIL. CODE §§ 2871–2876 (West 2018) (“Whenever telephone calls are placed through the use of an automatic dialing-announcing device, the device may be operated only after an unrecorded, natural voice announcement has been made to the person called by the person calling.”).

43. CAL. BUS. & PROF. CODE § 17538.41(a)(1) (“[N]o person, entity conducting business, candidate, or political committee in this state shall transmit, or cause to be transmitted, a text message advertisement to a mobile telephony services handset, pager, or two-way messaging device that is equipped with short message capability or any similar capability allowing the transmission of text messages.”).

44. *Id.* § 17529.5(a) (regulating unsolicited commercial e-mails with misleading or falsified headers or information); CAL. BUS. & PROF. CODE § 17538.45(f)(1) (West 2018) (giving e-mail service provider the right to sue those who send spam from its network or to its subscribers).

45. CAL. PEN. CODE § 502 (West 2018) (“It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.”).

plate recognition systems to smart TVs, from RFID tags to e-readers, and from automobile “black boxes” to surveillance systems in rental cars.⁴⁶

5. Other Modality-Focused Laws

Aside from the TCPA, CAN-SPAM, and the CFAA, a number of other federal laws have focused either on specific modes of communication or on narrow types of privacy problems. For example, the Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime punishable by up to 15 years in prison and fines up to \$250,000;⁴⁷ the Electronic Communications Privacy Act of 1986,⁴⁸ which updated the Federal Wiretap Act of 1968, encompassed interception of computer and other digital and electronic communications; and the Telemarketing Sales Rule established the National “Do Not Call” Registry.⁴⁹

Also, in addition to the California laws discussed above, there are a host of state laws which govern specific modalities or narrow privacy issues. For example, there are at least forty-five different state laws that govern some aspect of telephone solicitation, including a number of so-called “mini-TCPA” laws, which mirror federal legislation in their breadth.⁵⁰ There are also laws in all fifty states governing consent for recording calls, with twelve states requiring the consent of everyone involved in a phone conversation.⁵¹ In addition, there are state laws

46. See *Privacy Laws*, STATE OF CAL. DEP’T OF JUST. OFFICE OF THE ATT’Y GEN., <https://oag.ca.gov/privacy/privacy-laws> (last visited Oct. 28, 2018) [hereinafter *California AG Privacy Summary*].

47. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1028 (2006) and 28 U.S.C. § 994 (2006)); see *United States v. Karro*, 257 F.3d 112, 117 (2d Cir. 2001).

48. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

49. 16 C.F.R. §§ 310.1–310.9 (2018); see also *The Telemarketing Sales Rule*, FED. TRADE COMM’N CONSUMER INFO., <https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule> (last visited Feb. 17, 2019) (“The Federal Trade Commission’s Telemarketing Sales Rule (TSR) puts you in charge of the number of telemarketing calls you get at home. The TSR established the National Do Not Call Registry, which makes it easier and more efficient for you to reduce the number of unwanted telemarketing sales calls you get.”).

50. See Patricia Pattison & Anthony F. McGann, *State Telemarketing Legislation: A Whole Lotta Law Goin’ On*, 3 WYO. L. REV. 167, Appendix A (State Telemarketing Statutes) (2017); Dominique R. Shelton & David Carpenter, *Is Your Organization in Compliance with State Mini-TCPA Laws?*, ALSTON & BIRD (Oct. 7, 2014), <https://www.alston.com/-/media/files/insights/publications/2014/10/privacy--security-advisoryi-is-your-organization/files/view-advisory-as-pdf/fileattachment/14803-minitcpaadvisory.pdf>.

51. See, e.g., KRISTEN RASMUSSEN ET AL., REPORTERS COMMITTEE FOR FREEDOM PRESS, REPORTER’S RECORDING GUIDE (2012), <https://www.rcfp.org/wp-content/uploads/imported/RECORDING.pdf>.

governing connected televisions, employee email communications, information held by Internet service providers, and e-readers.⁵²

B. Content-Focused Laws

Aside from laws focused on a mode of communication or kind of document, other federal and state laws seek to regulate privacy in the context of specific types of data or industries. Just as the aforementioned laws seek to address a unique exigency related to a specific form of communication, these laws are intended to protect especially sensitive information.

1. The FCRA

Enacted in 1970, the Fair Credit Reporting Act (FCRA) has been amended a number of times, most notably in the Consumer Credit Reporting Reform Act of 1996 (the 1996 Amendments) and the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).⁵³ As amended, the statute is designed broadly, to protect “information collected by consumer reporting agencies such as credit bureaus, medical information companies, and tenant screening services.”⁵⁴ Among other things, the FCRA provides consumers with a bundle of core rights: (1) to know what is in a credit file, (2) to ask for a credit score, (3) to dispute incomplete or inaccurate information, (4) to give consent before reports are provided to employers, and (5) to seek redress in the event of identity theft.⁵⁵

The FCRA may be enforced by states and the FTC.⁵⁶ In addition, the FCRA provides individuals with a private right of action, and the ability to recover actual or statutory damages ranging between \$100 and \$1,000, attorney’s fees, costs, and punitive damages if the violation was willful.⁵⁷

52. See *California AG Privacy Summary*, *supra* note 46; *State Laws Related to Privacy*, NAT’L CONF. OF STATE LEGISLATURES (Feb. 8, 2019), <http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-Internet-privacy.aspx> [hereinafter *NCSL Privacy Summary*].

53. 15 U.S.C. § 1681 (2018); see also FED. TRADE COMM’N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS (2011), <https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrrreport.pdf>.

54. *Fair Credit Reporting Act*, FED. TRADE COMM’N <https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act> (last visited Feb. 17, 2019).

55. *A Summary of Your Rights Under the Fair Credit Reporting Act*, FED. TRADE COMM’N, <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> (last visited Feb. 17, 2019).

56. *Id.*

57. Meir Feder & Rajeev Muttreja, *Understanding the Fair Credit Reporting Act*, PRACTICAL LAW, Apr.–May 2016, at 48, 52, <http://www.jonesday.com/files/Publication/>

2. IPAA

Like the FCRA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), together with the Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), is intended to protect an especially sensitive category of data: the health information of patients.⁵⁸ Passed in 1996, HIPAA was the first federal statute to regulate private healthcare.⁵⁹

Generally, HIPAA applies to all so-called “covered entities,” which include health plans, healthcare clearinghouses, and any healthcare provider that transmits health information in electronic form in connection with certain transactions affected by HIPAA,⁶⁰ as well as “business associates,” or entities that act on behalf of, or provide certain services to, a covered entity, where those acts or services involve “individually identifiable health information.”⁶¹ “Individually identifiable health information” is defined as information including demographic data that relates to an individual’s physical or mental health condition, provision of healthcare to the individual, or payment for the provision of health care to the individual.⁶²

HIPAA limits permitted uses and disclosures to the following: (1) disclosures to the individual, unless required for access or accounting of disclosures; (2) as required for treatment, payment, and care operations; (3) where individuals agree to disclosure; (4) where disclosure is “incidental” to an otherwise lawful disclosure; (5) for public interest purposes; and (6) where information is disclosed as part of a “limited data set.”⁶³

e42f45d6-a8c6-43fc-a3d7-3fd302b447c6/Presentation/PublicationAttachment/1d5beeac-8049-48ec-9832-a45699daedeb/Understanding%20the%20FCRA.pdf.

58. 42 U.S.C. § 1320d (2018); see also *General Overview of Standards for Privacy of Individually Identifiable Health Information*, U.S. DEP’T OF HEALTH & HUMAN SERVS. (Apr. 3, 2003), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/general-overview/index.html>.

59. *It’s Hip to Be Fair, HIPAA: What It Says, What It Means, What We Do, Presented to American Bar Association ERR and EEO Committees*, JONES DAY (Mar. 2004), <http://www.jonesday.com/Its-Hip-to-Be-Fair-HIPAA-What-It-Says-What-It-Means-What-We-Do-Presented-to-American-Bar-Association-ERR-and-EEO-Committees-03-01-2004/>.

60. See *General Overview of Standards for Privacy of Individually Identifiable Health Information*, *supra* note 58.

61. *Id.*

62. *What Is Individually Identifiable Health Information?*, HIPAA JOURNAL (Jan. 11, 2018), <https://www.hipaajournal.com/individually-identifiable-health-information/>.

63. See JONES DAY, *supra* note 59.

3. The GLBA

Aside from the FCRA and HIPAA, another prominent piece of federal privacy legislation which is aimed at a specific industry or type of information is the Gramm-Leach-Bliley Act (GLBA).⁶⁴ Broadly speaking and in the words of the FTC, the GLBA “requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data.”⁶⁵

GLBA violators may be liable for civil and criminal penalties, including fines of \$100,000 for each violation and imprisonment for up to five years.⁶⁶

4. Content-Focused Laws in California

As on the federal level, California also has a number of privacy laws aimed at protecting particularly sensitive information. For a few examples, the Consumer Credit Reporting Agencies Act, like the FCRA, places restrictions on credit reporting agencies;⁶⁷ the Financial Information Privacy Act, like GLBA—though in more stringent fashion—prohibits financial institutions from sharing or selling personally identifiable nonpublic information;⁶⁸ the Confidentiality of Medical Information Act, like HIPAA, restricts the use and disclosure of patients’ medical information;⁶⁹ and the Credit Card Full Disclosure Act

64. 15 U.S.C. § 6802 (2018).

65. *Gramm-Leach-Bliley Act*, FED. TRADE COMM’N, <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act> (last visited Feb. 17, 2019).

66. 18 U.S.C. §§ 2721–2725 (West 1994 & Supp. 1994) (regulates the disclosure of personal information contained in the records of state motor vehicle departments); *Reno v. Condon*, 528 U.S. 141, 143 (2000); 18 U.S.C. § 2710(b) (2018) (limiting the conditions under which video rental or sales stores can disclose personally identifiable information, including viewing history).

67. See CAL. CIV. CODE § 1785.1(c) (West 2018) (“The Legislature finds and declares as follows: . . . (c) There is a need to ensure that consumer credit reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer’s right to privacy.”).

68. See CAL. FIN. CODE § 4051 (West 2004) (“(a) The Legislature intends for financial institutions to provide their consumers notice and meaningful choice about how consumers’ nonpublic personal information is shared or sold by their financial institutions. (b) It is the intent of the Legislature in enacting the California Financial Information Privacy Act to afford persons greater privacy protections than those provided in Public Law 106-102, the federal Gramm-Leach-Bliley Act, and that this division be interpreted to be consistent with that purpose.”).

69. See CAL. CIV. CODE § 56.07 (West 2001).

allows credit card holders to opt out of the sharing of information by credit card companies.⁷⁰

C. Laws Protecting Children

1. COPPA

Aside from privacy laws aimed at specific modalities or types of information, the third main category of privacy laws in the U.S. include laws protecting particularly vulnerable data subjects—children.⁷¹ On the federal level, the Children’s Online Privacy Protection Act (COPPA),⁷² including the COPPA Rule,⁷³ is the primary law protecting children’s privacy online. Passed in 1998, COPPA makes it unlawful for website operators to collect, use, or disclose children’s information without verifiable parental consent.⁷⁴

COPPA gives states and federal agencies, including most notably the FTC, authority to enforce compliance.⁷⁵ In addition, civil penalties for violation of the COPPA Rule can be as high as \$41,484 per violation.⁷⁶

2. California Laws Protecting Children

Finally, California has what is probably the nation’s most robust regime aimed at protecting children’s online privacy. The Privacy Rights for California Minors in the Digital World Act restricts certain types of marketing to minors.⁷⁷ It also allows minors who are registered users of an operator’s site or service to request removal of personal content.⁷⁸ California Education Code Sections 49073.1 and 49073.6 and the Student Online Personal Information Protection Act are designed to protect student privacy.⁷⁹

70. *See id.* § 1748.12 (West 2002).

71. *See, e.g.,* CAL. PEN. CODE § 964 (West 2003) (protecting personal information of witnesses and victims). Although this section focuses on children, the group most often given special privacy law protection, there are other laws aimed at protecting other sensitive data subjects.

72. *See* 15 U.S.C. §§ 6501–6506 (2018).

73. *See* 16 C.F.R. § 312 (2019).

74. 15 U.S.C. § 6502(b)(1)(A)(ii).

75. *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM’N (Mar. 20, 2015), <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>.

76. *Id.*

77. CAL. BUS. & PROF. CODE §§ 22580–22582 (West 2015).

78. *See id.*

79. CAL. EDUC. CODE §§ 49073.1, 49073.6 (West 2016); *see* CAL. BUS. & PROF. CODE § 22584 (West 2016).

3. Other Laws Protecting Children

In addition to COPPA, the Family Educational Rights and Privacy Act of 1964 protects the privacy of student education records,⁸⁰ and provisions of HIPAA prohibit third parties from sharing a minor's personal information without the consent of the parent.⁸¹ Likewise, the Children's Internet Protection Act, enacted in 2000, regulates children's access to obscene or harmful content over the Internet.⁸² Aside from the California laws discussed below, the Delaware Online Privacy and Protection Act (DOPPA), which strictly regulates advertisements on websites directed at children, represents another state law effort to protect children online.⁸³

II. PRIVACY LAW IN EUROPE

For decades, European privacy law has offered a stark contrast to the content-, modality-, and subject-focused data regime in the United States. This contrast is rooted in underlying norms and conflicting values about the importance of free enterprise and flow of information on one hand and the individual's privacy on the other.⁸⁴ Whereas legislators in the U.S. "tend[] to emphasize the free flow of information and minimal government regulation," European focus has traditionally been "first and foremost on individual privacy protection as a basic human right."⁸⁵

80. 20 U.S.C. § 1232g (2018). For an article arguing that privacy laws aimed at protecting children simply confer rights on children's parents and are thus insufficient, especially in the age of social media, see Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839 (2017).

81. *Can a Minor Child's Doctor Talk to the Child's Parent About the Patient's Mental Health Status and Needs?*, U.S. DEP'T. OF HEALTH & HUMAN SERVS. (Sept. 12, 2017), <https://www.hhs.gov/hipaa/for-professionals/faq/2092/can-minor-childs-doctor-talk-childs-parent-about-patients-mental-health-status-and-needs.html>.

82. Consolidated Appropriations Act of 2001, Pub. L. No. 106-554, 114 Stat. 2763A-335 (2001).

83. DEL. CODE ANN. tit. 6, §§ 1201C–1206C (2015).

84. Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1989 (2013) ("U.S. information privacy regulation was based on liberal norms and market forces, while the EU's information privacy regulations were based on 'social-protection norms' according to which 'data privacy is a political imperative anchored in fundamental human rights protection.'") (quoting Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1347 (2000)).

85. P. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 L. & POL'Y INT'L BUS. 275, 277 (1998) ("Consistent with its free market emphasis, the United States takes a very sectoral approach to data protection. Most U.S. legislation focuses on the public sector, leaving the private sector to rely on voluntary compliance. In contrast, Europe has developed more omnibus standards to be applied to both government and private actors."); see also *infra* note 89.

A. The EU Data Protection Directive

Privacy laws in Europe stretch back a number of years,⁸⁶ but the first really significant and truly continental step towards comprehensive data protection and privacy legislation, passed on October 24, 1995, was Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, also known as “the Data Protection Directive” or simply, “the Directive.”⁸⁷ Despite the long-running European emphasis on privacy, discussed above, the Directive was enacted with two competing goals in mind: (1) instituting a streamlined framework to help secure the free movement of data across internal EU borders; and (2) enshrining basic personal privacy and data security guarantees.⁸⁸

Most notably, the Directive provided EU member states and private companies with a harmonized set of best practices as well as privacy and data protection principles. The Directive, in other words, was the first major piece of legislation to articulate broad, overarching terms regarding internet privacy. Expressly citing Article 8 of the European Convention for the Protection of Human Rights (ECPHR), drafted in 1950 and in force since 1953,⁸⁹ the Directive declared that “the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy.”⁹⁰

86. Neil Robinson et al., RAND CORP., REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 6 (2009), https://www.rand.org/pubs/technical_reports/TR710.html [hereinafter RAND REPORT] (“At the European level, the protection of privacy as an essential human right has been encased in a number of regulatory texts, most of which came into being after the Second World War.”); Monahan, *supra* note 85, at 283 (“Fueled by memories of the Third Reich’s use of personal data to track targeted populations, European nations have long treated privacy as a fundamental human right.”).

87. See Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN> [hereinafter Directive].

88. EU Data Protection Directive, ELEC. PRIVACY INFO. CTR., https://www.epic.org/privacy/intl/eu_data_protection_directive.html (last visited Feb. 15, 2019).

89. Article 8 provides that “[e]veryone has the right to respect for his private and family life, his home and his correspondence.” Convention for the Protection of Human Rights and Fundamental Freedoms, Apr. 11, 1950, E.T.S. No. 005, https://www.echr.coe.int/Documents/Convention_ENG.pdf [hereinafter ECPHR]. See Aisha Gani, *What Is the European Convention on Human Rights?*, GUARDIAN (Oct. 3, 2014), <https://www.theguardian.com/law/2014/oct/03/what-is-european-convention-on-human-rights-echr>.

90. See Directive, *supra* note 87, at 32.

Although the Directive was a massive step forward for privacy in the EU,⁹¹ it was ultimately proven to be inadequate to the challenges posed by the Internet's rapid evolutions.⁹² Among other weaknesses, the Directive ultimately left it to member states to implement and enforce their own national privacy legislation under the Directive's overarching standards.⁹³ But the Directive's narrower territorial scope hampered enforcement efforts against entities located outside the EU, most notably large U.S. companies like Google and Facebook—companies often seen by European privacy advocates as the chief violators of European privacy norms.⁹⁴

B. GDPR

Following years of drafting and debate, the EU published GDPR in May 2016; the legislation went into effect in all EU Member states as of May 25, 2018.⁹⁵ While a number of provisions and principles stayed the same as the Directive, GDPR sweeps in a number of new data collectors and processors, as well as data subjects, and has vastly stronger enforcement mechanisms. In a lecture in January 2017, UK Information Commissioner Elizabeth Denham summed up the transition this way:

91. RAND REPORT, *supra* note 86, at 8 (“While the Directive was not conceptually innovative, it has had a very powerful impact in the EU and can be credited with creating a binding and harmonised framework for data protection principles in all Member States.”).

92. B.J. Koops, *The Trouble with European Data Protection Law*, 4 INT’L DATA PRIVACY L. 250, 250 (2014) (“The trouble with the [European data protection] law, as with Hitchcock’s Harry, is that it’s dead. What the statutes describe and how the courts interpret this has usually only a marginal effect on data-processing practices.”).

93. Monahan, *supra* note 85, at 286.

94. Despite the Directive’s limitations, the European Court of Justice had already begun developing rules that extended European privacy laws abroad. *EU General Data Protection Regulation—Key Changes*, DLA PIPER, <https://www.dlapiper.com/en/us/focus/eu-data-protection-regulation/key-changes/> (last visited Feb. 15, 2019) (“Europe’s highest court, the Court of Justice of the European Union (the CJEU) has been developing jurisprudence on this concept, recently finding (*Google Spain SL, Google Inc. v. AEPD, Mario Costeja Gonzalez* (C-131/12)) that Google Inc. with EU based sales and advertising operations (in that particular case, a Spanish subsidiary) was established within the EU. More recently, the same court concluded (*Weltimmo v NAIH* (C-230/14)) that a Slovakian property website was also established in Hungary and therefore subject to Hungarian data protection laws.”).

95. Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> [hereinafter GDPR]; JONES DAY, GENERAL DATA PROTECTION REGULATION GUIDE (2004), http://www.jonesday.com/files/upload/GDPR%20Pocket%20Guide%20A5%2004_17_18%20ENGLISH.pdf [hereinafter JONES DAY GDPR GUIDE].

“There’s a lot in the GDPR you’ll recognise from the current law, but make no mistake, this one’s a game changer for everyone.”⁹⁶

Perhaps most importantly, GDPR’s wide territorial scope has companies all over the world—and in the U.S. in particular—scrambling to adapt themselves to European privacy norms.⁹⁷ GDPR applies not only to businesses “established” in the EU, but also to any controller or processor conducting activities related to the offering of goods and services to data subjects “in the Union.”⁹⁸ The GDPR also applies to the monitoring of such data subjects’ behavior.⁹⁹ In other words, GDPR has nothing to do with citizenship or protecting the rights of Europeans, *per se*. Proceeding from a right to privacy that is discussed in Article 1 in universal terms, the law aims to protect anyone in Europe, even tourists.¹⁰⁰

96. Elizabeth Denam, UK Info. Comm’r, Address at the Meeting of the Institute of Chartered Accountants in England and Wales (Jan. 17, 2017) (transcript available at <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/>).

97. Jeong, *supra* note 15.

98. Specifically, GDPR Art. 3 provides as follows:

(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

(3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

GDPR, *supra* note 95, at 32.

99. *Id.*

100. *The GDPR’s Reach: Material and Territorial Scope Under Articles 2 and 3*, WILEY REIN LLP (May 2017), https://www.wileyrein.com/newsroom-newsletters-item-May_2017_PIF-The_GDPRs_Reach-Material_and_Territorial_Scope_Under_Articles_2_and_3.html (“Notably, Article 3(2) applies to the processing of personal data of any individual ‘in the EU.’ The individual’s nationality or residence is irrelevant. The GDPR protects the personal data of citizens, residents, tourists, and other persons visiting the EU. So long as an individual is in the EU, any personal information of that person collected by any controller or processor who meets the requirements of Article 3(2) is subject to the GDPR. Where Article 3(2) applies, controllers or processors must appoint an EU-based representative.”); see also Tess Blair et al., *Whose Data Is*

Additionally, GDPR expands the definition of “personal data,” directly regulates processors for the first time, adds a new data protection principle (“accountability”), introduces new data breach notification requirements, and requires Data Protection Officers to be appointed under certain circumstances.¹⁰¹ GDPR also contains a number of required disclosures for privacy policies including, among others, the identity and contact details of data “controllers”;¹⁰² the purposes of the data “processing” and the legal bases for doing so;¹⁰³ categories of personal data being processed;¹⁰⁴ categories of recipients receiving personal data;¹⁰⁵ the amount of time personal data is retained, or the factors in making that determination;¹⁰⁶ and the existence of specific consumer rights, such as the right to access, correct, and request deletion of data, as well as the right to lodge a complaint with a supervisory authority.¹⁰⁷

GDPR introduces new and remarkably tough enforcement mechanisms. Most notably, GDPR introduces revenue-based fines of up to 4% of a company’s global revenue.¹⁰⁸ Although it is still unclear, this calculation may include revenues of group companies, which have nothing to do with the collection or processing of the data in question.¹⁰⁹ In addition to revenue-based fines, Article 58 gives broad “investigative” and “corrective” powers to EU supervisory authorities and makes it much easier for data subjects to bring their own claims against controllers and processors.¹¹⁰

Finally, as with the “Safe Harbor” regime that was in place under the Directive, U.S. companies may certify GDPR compliance by registering with the U.S. Department of Commerce under the EU-U.S. and

Protected Under the GDPR?, LEXOLOGY (June 20, 2018), <https://www.lexology.com/library/detail.aspx?g=0dc9663d-ac3b-438e-adcd-1415a45f99ca>.

101. See GDPR, *supra* note 95, at 33–35; JONES DAY GDPR GUIDE, *supra* note 95, at 1.

102. GDPR, *supra* note 95, at 40. GDPR defines a data “controller” as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.” *Id.* at 33.

103. *Id.* at 40. GDPR defines data “processing” as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.” *Id.* at 33.

104. *Id.* at 41.

105. *Id.*

106. *Id.*

107. *Id.*

108. See *id.* at 82–83.

109. See JONES DAY GDPR GUIDE, *supra* note 95.

110. GDPR, *supra* note 95, at 69–70.

Swiss-U.S. Privacy Shield Frameworks.¹¹¹ In order to qualify, U.S. companies must develop a conforming privacy policy, identify an independent recourse mechanism, and self-certify through the Department of Commerce website.¹¹² As a result, participating organizations are deemed to have “adequate” privacy protection under GDPR.¹¹³

As of the time of this writing, it still remains to be seen what effect GDPR will have on European and American companies. Although privacy campaigner Max Schrems has already initiated at least one high profile lawsuit against Facebook and Google, EU officials have yet to levy any fines.¹¹⁴

III. THE CALIFORNIA CONSUMER PRIVACY ACT

Just as the starting point for discussion of European privacy law is the ECPHR and the individual right to privacy, the starting point for discussion of California privacy law is Article I, Section 1 of the California Constitution, which provides that “[a]ll people are by nature free and independent and have inalienable rights . . . enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*.”¹¹⁵ California is one of only ten states to enshrine privacy as an enumerated right in its constitution.¹¹⁶ Perhaps in part because of this explicit constitutional right, California privacy law, even prior to the CCPA, has traditionally been far more elaborate—and strict—than that of any other state. In fact, the California Attorney General website lists 118 different “privacy” laws.¹¹⁷ Nevertheless, in spite of this broad constitutional protection, and in spite of the California legislature’s evident willingness to enact privacy

111. See *Privacy Shield Framework*, INT’L TRADE ADMIN., <https://www.privacyshield.gov/welcome> (last visited Feb. 24, 2019).

112. *U.S. Businesses*, INT’L TRADE ADMIN., <https://www.privacyshield.gov/US-Businesses> (last visited Feb. 24, 2019).

113. *Benefits of Participation*, INT’L TRADE ADMIN., <https://www.privacyshield.gov/article?id=Benefits-of-Participation> (last visited Feb. 24, 2019).

114. Derek Scally, *Max Schrems Files First Cases Under GDPR Against Facebook and Google*, IRISH TIMES (May 25, 2018), <https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177>; Michele Gorman, *3 Things That Have (or Haven’t) Happened Since the GDPR*, LAW360 (July 18, 2018), <https://www.law360.com/articles/1061080/3-things-that-have-or-haven-t-happened-since-the-gdpr>.

115. CAL. CONST. art. I, § 1 (emphasis added). See also J. Clark Kelso, *California’s Constitutional Right to Privacy*, 19 PEPP. L. REV. 327 (1992), <https://www.law.berkeley.edu/wp-content/uploads/2016/12/Kelso-Californias-Constitutional-Right-to-Privacy.pdf>.

116. *Privacy Protections in State Constitutions*, NAT’L CONFERENCE OF STATE LEGISLATURES (Nov. 7, 2018), <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx>.

117. *California AG Privacy Summary*, *supra* note 46.

legislation, the extant privacy laws in California are still narrowly tailored and can fit into the three categories discussed above: laws that are modality-focused, content-focused, or aimed at protecting children or other vulnerable groups.

Prior to the CCPA, the lone exception to this framework in California was the California Online Privacy Protection Act (CalOPPA), effective in 2004, which was already the broadest internet privacy law in the United States.¹¹⁸ Among other things, CalOPPA—the first law in the nation to do so—requires commercial websites and online services to post a privacy policy.¹¹⁹ The privacy policy must be posted “conspicuously,” must state clearly what information is collected, and who that information is shared with.¹²⁰ In 2013, the law was amended to require website privacy policies to disclose whether operators respond to “Do Not Track” signals.¹²¹ However, CalOPPA is focused more on transparency than on empowering consumers to take back control of their data. By contrast, the CCPA is more focused on the issue of consumer control.

A. *The Ballot Initiative*

Notwithstanding any other comparisons to European privacy law, the CCPA’s origins, at least, are uniquely Californian. According to a number of interviews he has given, Alastair Mactaggart, the 51-year-old Bay Area real estate mogul behind the ballot initiative, first became “concerned about data privacy” while talking to a Google engineer at a cocktail party.¹²² Reportedly, Mactaggart asked the engineer whether he should be “worried” about the information companies like Google were collecting about users.¹²³ According to Mactaggart, the engineer replied,

118. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014).

119. *California Online Privacy Protection Act*, CONSUMER FED’N OF CAL. EDUC. FOUND. (July 29, 2015), <https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/>.

120. *Id.*

121. *California Amends Online Privacy Policy Law to Require Tracking Disclosures*, HUNTON ANDREWS KURTH PRIVACY & INFO. SECURITY LAW BLOG (Sept. 30, 2017), <https://www.huntonprivacyblog.com/2013/09/30/california-amends-online-privacy-policy-law-to-require-tracking-disclosures/>.

122. Daisuke Wakabayashi, *Silicon Valley Faces Regulatory Fight on Its Home Turf*, N.Y. TIMES (May 13, 2018), <https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html>.

123. Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. TIMES MAG. (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>.

“If people just understood how much we knew about them, they’d be really worried.”¹²⁴

Mactaggart then convinced Rick Arney, a finance executive who had worked as a legislative analyst in the California State Senate, to help him with a ballot initiative.¹²⁵ Neither of the pair were especially savvy in privacy: they added Mary Stone Ross, who previously worked at the Central Intelligence Agency and had been legal counsel for the House of Representatives Intelligence Committee.¹²⁶

As any California resident knows, the ballot measure process can play a high-profile and often contentious place in California politics.¹²⁷ Generally, there are two ways to put a ballot measure up for a popular vote: (1) the legislature may place constitutional amendments, bond measures, and proposed changes in existing law on the ballot; and (2) any California voter can put on the ballot a referendum—which submits to voters a statute already passed by the legislature—or an initiative that proposes, or “initiates,” a statute or constitutional amendment.¹²⁸ To qualify an initiative, organizers must secure 365,880 votes.¹²⁹ According to reports, Mactaggart, Arney, and Ross submitted more than 600,000.¹³⁰ Not surprisingly, a number of major tech companies, including Google and Facebook, publicly opposed the initiative and even created an organization to that end: “The Committee to Protect California Jobs.”¹³¹

124. *About Us*, CALIFORNIANS FOR CONSUMER PRIVACY, <https://www.caprivacy.org/about-us> (last visited Feb. 24, 2019).

125. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), <https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html>.

126. *Id.*

127. See Hillel Aron, *How California’s Ballot Measure Process Got So Kooky*, L.A. WEEKLY (Oct. 22, 2016), <http://www.laweekly.com/news/how-californias-ballot-measure-process-got-so-kooky-7526677> (discussing, *inter alia*, Proposition 13, passed in 1978, which drastically reduced property taxes and required two-thirds voter support for future tax increases; Proposition 64, defeated in 1986, which would have added AIDS to the state’s list of communicable diseases; Proposition 161, defeated in 1992, which would have legalized assisted suicide; and Proposition 8, passed in 2008, which banned same-sex marriage).

128. See *Ballot Measures*, CAL. SEC’Y OF STATE, <http://www.sos.ca.gov/elections/ballot-measures/> (last visited Feb. 15, 2019).

129. See *How to Qualify an Initiative: Statewide Ballot Initiative Guide*, CAL. SEC’Y OF STATE, <http://www.sos.ca.gov/elections/ballot-measures/how-qualify-initiative/> (last visited Feb. 15, 2019).

130. Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, WIRED (June 28, 2018, 5:57 PM), <https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/>.

131. See Julia B. Jacobson et al., *Frequently Asked Questions About the California Consumer Privacy Act of 2018*, K&L GATES: “STAY INFORMED” BLOG (July 31, 2018), <http://www.klgates.com/frequently-asked-questions-about-the-california-consumer-privacy-act-of-2018-ccpa-07-31-2018/>.

As originally drafted, the initiative granted consumers three core rights: (1) the right to know what data companies have collected about them; where it is sourced from; and how it is being used, sold, or disclosed; (2) the right to “opt out” of the sale or sharing of their data for business purposes, or the right for consumers under 16 years old not to have their information sold absent their or their parents’ “opt in”; and (3) the right to sue companies that violate the law.¹³² Summing up these rights, the website launched for the initiative declared the following mission: “Your life is not their business.”¹³³

In response to a request from concerned legislators that the initiative be withdrawn, the initiative’s drafters set a deadline of June 28, 2018 for the legislature to pass comparable privacy legislation—or else face the initiative appearing on the November ballot with risk of passage by the voters in November.¹³⁴ Critically, the initiative would have provided lawmakers with little wiggle room to make changes to the law: unlike regular legislation, ballot initiatives cannot be amended by the legislature.¹³⁵ Faced with this reality, the legislature hastily introduced A.B. 375, a bill substantially similar to the initiative, which passed on the same day as the deadline.¹³⁶ The bill was passed under the same name as the ballot initiative: The California Consumer Privacy Act.

B. *The California Consumer Privacy Act*

Except for a much more limited private right of action and a key whistleblower provision included in the original initiative, A.B. 375 preserves the core rights enshrined by the initiative’s drafters and adds a fourth key right: the right to have a business delete a consumer’s personal

132. Mary Ross & Alastair Mactaggart, *The Consumer Right to Privacy Act of 2018—Version 2*, CAL. OFFICE OF THE ATT’Y GEN. (Nov. 17, 2017), <https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf> [hereinafter *Ballot Initiative*]. See also *About the California Consumer Privacy Act*, CALIFORNIANS FOR CONSUMER PRIVACY, <https://www.caprivacy.org/about> (last visited Feb. 15, 2019).

133. CALIFORNIANS FOR CONSUMER PRIVACY, *supra* note 124.

134. See *id.* (“In mid-May 2018, we were contacted by Senator Robert Hertzberg and Assemblyman Ed Chau, of the California Legislature, to see if I would withdraw the initiative from the ballot, if the California Legislature passed a law addressing our privacy concerns. We replied that we would withdraw the initiative, if the Legislature passed a law replicating all its critical components, prior to our statutory deadline to withdraw, which was 5PM on Thursday June 28th, 2018.”).

135. Kristen J. Matthews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER ROSE LLP: PRIVACY LAW BLOG (July 13, 2018), <https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/>.

136. See Heather Kelly, *California Passes Strictest Online Privacy Law in the Country*, CNN BUS. (June 29, 2018, 12:03 PM), <https://money.cnn.com/2018/06/28/technology/california-consumer-privacy-act/index.html>.

information, with some exceptions.¹³⁷ Below is a brief overview of the law's key components.

1. Who (and What) is Covered by the CCPA?

Generally, the CCPA applies to a “business,” defined as any for-profit entity “that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds”: brings in annual gross revenue “in excess of \$25,000,000”; buys, sells, receives, or shares, for commercial purposes, the personal information of 50,000 or more “consumers, households, or devices”; or derives 50% or more of its annual revenues from selling consumers’ personal information.¹³⁸ The definition also includes “[a]ny entity that controls or is controlled by a business, as defined in [the main “business” definition], and that shares common branding with the business.”¹³⁹

The CCPA defines a “consumer” as “a natural person who is a California resident,”¹⁴⁰ and “personal information” as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”¹⁴¹ The CCPA also lists a number of “personal information” examples, including without limitation: names, aliases, postal addresses, IP addresses, social security numbers, and “other similar identifiers,” together with biometric information, geolocation data, “professional or employment-related information,” and “education information.” This definition, and the Act as a whole, “apply to the collection and sale of all personal information collected by a business from consumers,” whether in electronic, paper, or other form.¹⁴²

137. CAL. CIV. CODE § 1798.105 (West 2018).

138. *Id.* § 1798.140(c)(1). This definition is broader than the initiative, which set the revenue floor at \$50,000,000 and the floor for “consumers or devices” at \$100,000. *Ballot Initiative*, *supra* note 132, at 8.

139. *Id.* § 1798.140(c)(2). According to the International Association of Privacy Professionals (IAPP), the law will likely affect more than half a million U.S. companies, “the vast majority of which are small- to medium-sized enterprises.” Rita Heimes, *New California Privacy Law to Affect More Than Half a Million U.S. Companies*, IAPP (July 2, 2018), <https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/>.

140. “Resident” is defined according to state tax regulations. CAL. CIV. CODE § 1798.140(g).

141. *Id.* § 1798.140(o)(1). The Act also expressly excludes certain information covered by other statutes, including HIPAA, the FCRA, the GLBA, and the DPPA. *Id.* § 1798.145.

142. This title is intended to *further the constitutional right of privacy* and to supplement existing laws relating to consumers’ personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of

Critically, the Act also excludes certain personal information covered by federal privacy laws, namely HIPAA, the FCRA, the GLBA, and the DPPA. In cases of overlap with HIPAA, the Act “shall not apply to protected or health information that is collected by a covered entity,” as “protected health information” and “covered entity” are defined in the HIPAA Privacy Rule.¹⁴³ And in the cases of overlap with the FCRA, the Act “shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report,” and “use of that information is limited by the [FCRA].”¹⁴⁴ If there is overlap with the GLBA and DPPA, the CCPA continues to apply unless it is “in conflict” with the federal statute.¹⁴⁵ The Act also excludes “publicly available information” from the “personal information” definition, though, as discussed below, what is “publicly available” is still vague.¹⁴⁶

Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are *not limited to information collected electronically or over the Internet*, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers’ personal information should be construed to harmonize with the provisions of this title, but *in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.*

Id. § 1798.175 (emphasis added).

143. *Id.* § 1798.145(c).

144. *Id.* § 1798.145(d).

145. *Id.* § 1798.145(e)–(f).

146. The Act defines “publicly available” as “information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information,” and excludes information that is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained”; information that is “deidentified or aggregate consumer information” is also excluded. *Id.* § 1798.140(o)(2). “Aggregate consumer information” means “information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.” It “does not mean one or more individual consumer records that have been deidentified.” *Id.* § 1798.140(a). “Deidentified” means “information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. (2) Has implemented business processes that specifically prohibit reidentification of the information. (3) Has implemented business processes to prevent inadvertent release of deidentified information. (4) Makes no attempt to reidentify the information.” *Id.* § 1798.140(h).

2. What Specific Rights Are Conferred on Consumers?

Sections 1798.100–1798.125 convey a number of specific rights on consumers. Under 1798.100, consumers have “the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.”¹⁴⁷ In response to these “verifiable consumer requests,” the business must provide this information free of charge.¹⁴⁸

Under Section 1798.105, “[a] consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”¹⁴⁹ Following such request, the business must delete the information from its own records, as well as the records of its “service providers.”¹⁵⁰ However, the Act lists some exceptions to this requirement: where retention of personal information is necessary to detect security incidents or protect against fraud, where necessary to comply with a legal obligation, or where such retention enables “solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business.”¹⁵¹

The Act also exempts from the deletion requirement businesses engaged in “public or peer-reviewed scientific, historical, or statistical research . . . when the businesses’ deletion of the information is likely to render impossible or seriously impair the achievement of such research”¹⁵² Elsewhere in the Act, “research” is defined as “scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public

147. *Id.* § 1798.100.

148. *Id.* § 1798.100(d) (“A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section.”).

149. *Id.* § 1798.105.

150. *Id.* § 1798.105(c).

151. *Id.* § 1798.105(d). Although California had already enshrined a “right to be forgotten” or a “right to erasure” in the “Online Eraser” law, which took effect on January 1, 2015, this right only applied to minors under the age of 18. CAL. BUS. & PROF. CODE § 22580 *et seq.* See also Rahul Kapoor & W. Reece Hirsch, *Get to Know California’s ‘Online Eraser’ Law*, MORGAN LEWIS: TECH & SOURCING (July 12, 2016), <https://www.morganlewis.com/blogs/sourcing/atmorganlewis/2016/07/get-to-know-californias-online-eraser-law>. Nevertheless, despite no U.S. legal requirement to do so, it is not unusual for American businesses to allow users to request deletion. See, e.g., Chris Smith, *How to Delete Your Facebook Account and Reclaim Your Data*, N.Y. POST (Mar. 20, 2018), <https://nypost.com/2018/03/20/how-to-delete-your-facebook-account-and-reclaim-your-data/>. But see *Privacy Policy*, APPLE INC. (May 22, 2018), <https://www.apple.com/legal/privacy/en-ww/> (limiting users’ deletion rights where Apple is required to retain it for legitimate business purposes).

152. CAL. CIV. CODE § 1798.105(d)(6).

interest in the area of public health.”¹⁵³ The Act also requires that:

Research with personal information that may have been collected from a consumer in the course of the consumer’s interactions with a business’ service or device for other purposes shall be: (1) Compatible with the business purpose for which it was collected. (2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate . . . (3) Made subject to technical safeguards that prohibit reidentification . . . (4) Subject to business processes that specifically prohibit reidentification . . . (5) Made subject to business processes to prevent inadvertent release of deidentified information. (6) Protected from any reidentification attempts. (7) Used solely for research purposes that are compatible with the context in which the personal information was collected. (8) Not be used for any commercial purpose.¹⁵⁴

With respect to Section 1798.110, consumers have the right to request the following from businesses that *collect* their information: (1) categories of personal information collected; “(2) The categories of sources from which the personal information is collected. (3) The business or commercial purpose¹⁵⁵ for collecting or selling personal

153. *Id.* § 1798.140(s).

154. The Act defines “pseudonymize” or “pseudonymization” as “the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.” *Id.* § 1798.140(r).

155. “Business purpose” means “the use of personal information for the business’s or a service provider’s operational purposes, or other notified purposes.” That use must be “reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected.” Business purposes are: (1) “Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.” (2) The detection, prevention and prosecution of security incidents and “deceptive, fraudulent, or illegal activity. (3) Debugging to identify and repair errors that impair existing intended functionality. (4) Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer’s experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction. (5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider. (6) Undertaking internal research for technological development and demonstration. (7) Undertaking

information. (4) The categories of third parties with whom the business shares personal information. (5) The specific pieces of personal information it has collected about that consumer.” “Collect” is defined as “buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer’s behavior.”¹⁵⁶

Similarly, under Section 1798.115, consumers have the right to request the following from businesses that *sell* the consumer’s information: “(1) The categories of personal information the business collected about the consumer. (2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold . . . (3) The categories of personal information that the business disclosed about the consumer for a business purpose.”¹⁵⁷ “Sell” is defined broadly as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.”¹⁵⁸

Section 1798.120 provides that a “consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal

activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.” *Id.* § 1798.140(d).

Likewise, “commercial purposes” is defined as “to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.” It does not include “engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.” *Id.* § 1798.140(f).

156. *Id.* § 1798.140(e).

157. *Id.* § 1798.115.

158. *Id.* § 1798.140(t)(1). *But see id.* § 1798.140(t)(2) (excluding from the “sale” definition a number of scenarios, including where “(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party; (B) The business uses or shares an identifier . . . for the purposes of alerting third parties that the consumer has opted out of the sale of . . . personal information; (C) The business uses or shares with a service provider,” for business purposes, provided “(i) the business has provided notice that information [is] being used or shared” and “(ii) the service provider does not further collect, sell, or use the personal information”; and “(D) The business transfers to a third party the personal information as . . . part of a merger, acquisition, bankruptcy, or other transaction.”).

information.¹⁵⁹ This right may be referred to as the right to opt-out.”¹⁶⁰ This section also requires an affirmative “opt-in” for consumers under 16 years of age.¹⁶¹ The Act also requires that businesses “[m]ake available to consumers two or more designated methods for submitting requests for information required to be disclosed . . . including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.”¹⁶² The Act also provides that a business receiving a “verifiable consumer request”¹⁶³ for information or deletion, for example, must “[d]isclose and deliver the required information to a consumer free of charge within 45 days of receiving” the request.¹⁶⁴

Finally, Section 1798.125 provides that businesses “shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights.”¹⁶⁵ Example discrimination includes, but is not limited to: “(A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services . . . (C) Providing a different level or quality of goods or services to the consumer. (D) Suggesting the

159. *Id.* § 1798.120

160. *Id.* § 1798.120(a).

161. For consumers between 13 and 16, the consumer must opt in; for consumers under 13, the consumer’s parent or guardian must opt in. *Id.* § 1798.120(d)

162. *Id.* § 1798.130(a)(1).

163. *Id.* § 1798.130(a)(2). *See also id.* § 1798.140(y) (“[V]erifiable consumer request” means “a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to [Section 1798.185 of the Act] to be the consumer about whom the business has collected personal information.”).

164. *Id.* § 1798.130(a)(2). The Act provides further as follows:

The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business’s duty to disclose and deliver the information within 45 days of receipt of the consumer’s request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer’s account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer’s option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

Id.

165. *Id.* § 1798.125(a)(1).

consumer will receive a different price.”¹⁶⁶ The Act also provides, however, that nothing prohibits a business from charging different prices, or delivering different quality, if the prices or quality are “reasonably related to the value provided to the consumer by the consumer’s data.”¹⁶⁷ The Act also expressly permits businesses to “offer financial incentives, including payments to consumers as compensation,” for the collection, sale, or deletion of personal information.¹⁶⁸

3. What Must Businesses Disclose in Their Privacy Policies?

Under the Act, a business must “[d]isclose the following information in its online privacy policy or policies . . . and in any California-specific description of consumers’ privacy rights”¹⁶⁹: “A description of a consumer’s rights pursuant to Sections 1798.110, 1798.115, and 1798.125¹⁷⁰ and one or more designated methods for submitting requests” for information; “categories of personal information it has collected about consumers in the preceding 12 months;” categories of sources from which personal information has been collected in the preceding 12 months; the business or commercial purpose for collection or sale; categories of personal information it has sold or disclosed for a business purpose in the preceding 12 months; the consumer’s right to opt out of the sale of personal information; and the consumer’s right to request deletion of personal information.¹⁷¹ Additionally, “at or before the point of collection,” businesses must “inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.”¹⁷²

4. What Additional Notifications Are Required?

Aside from required privacy policy disclosures, the CCPA introduces two more notice requirements with the potential to have a tremendous impact. First, any business required to grant a consumer the right to opt-out of the sale of personal information must also “[p]rovide a clear and

166. *Id.*

167. *Id.* § 1798.125(a)(2).

168. *Id.* § 1798.125(b)(1).

169. “[I]f the business does not maintain those policies,” the disclosures may be posted on its Internet Web site. In any case, the information must be updated at least once every 12 months. *Id.* § 1798.130(a)(5).

170. The rights provided in Sections 1798.110, 1798.115, and 1798.125 are discussed above. See *supra* Section III.B.2.

171. CAL. CIV. CODE § 1798.130(a)(5).

172. *Id.* § 1798.100(b).

conspicuous link on the business's Internet homepage,¹⁷³ titled 'Do Not Sell My Personal Information,' to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information."¹⁷⁴

Second, the business must also include a description of consumers' opt-out rights, along with a separate link to the "Do Not Sell My Personal Information" webpage in its online privacy policy and in any California-specific description of consumers' privacy rights.¹⁷⁵

5. What Remedies Do Consumers Have?

As passed by the legislature, the broad private right of action included in the ballot initiative was removed. However, under Section 1798.150, "[a]ny consumer whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for": (1) statutory damages from \$100 to \$750 per consumer per incident, or actual damages, whichever is greater; (2) injunctive or declaratory relief; or (3) "[a]ny other relief the court deems proper."¹⁷⁶

However, the consumer's right to bring an action as described above is subject to the following requirements: (1) before initiating any action on an individual or class-wide basis, the consumer must provide the business with 30 days' written notice of the specific provisions of the CCPA the consumer alleges have been violated, which the business has a 30-day opportunity to cure; (2) the consumer must "notify the Attorney General within 30 days that the action has been filed;" and (3) "[t]he Attorney General, upon receiving such notice, within 30 days, shall do one of the following:" (A) "[n]otify the consumer of the Attorney General's intent to prosecute an action against the violation;" "[i]f the Attorney General does not prosecute within six months, the consumer may proceed with the action;" (B) "[r]efrain from acting within the 30 days, allowing the consumer to bring the action to proceed;" or (C)

173. *Id.* § 1798.140(l) ("'Homepage' means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, 'About,' 'Information,' or settings page, and any other location that allows consumers to review [required notices] before downloading the application.").

174. *Id.* § 1798.135(a)(1).

175. *Id.* § 1798.135(a)(2).

176. *Id.* § 1798.150(a)(1).

“[n]otify the consumer that the consumer shall not be permitted to proceed with the action.”¹⁷⁷

6. What Powers Does the Attorney General Have?

In addition to the above right of action, the California Attorney General can also enforce the Act, with civil penalties for violations as high as \$7,500 per violation.¹⁷⁸ Of the proceeds of any such lawsuits, 20% goes to a new “Consumer Privacy Fund,” which would fund further lawsuits against violators.¹⁷⁹ The remaining 80% goes to “the jurisdiction on whose behalf the action leading to the civil penalty was brought.”¹⁸⁰

The Act also provides that the Attorney General “shall solicit broad public participation” in writing regulations for the Act, including: (1) updating the personal information definition; (2) updating the definition of unique identifiers; (3) “[e]stablishing any exceptions necessary to comply with state or federal law”; (4) establishing additional rules governing consumer requests and opt-outs; (5) adjusting monetary thresholds for company revenue that subject a company to the Act; (6) establishing additional rules to ensure information and notices provided to consumers are easily understood by all consumers, including disabled consumers or foreign language speakers; and (7) establishing additional rules to further consumers’ privacy rights, with the goal of minimizing the administrative burden on consumers.¹⁸¹ The Attorney General may also pursue any other regulations “as necessary to further the purposes” of the Act.¹⁸²

IV. TOWARDS A EUROPEAN-STYLE PRIVACY REGIME?

A. *The CCPA, GDPR, and the Future of American Privacy Law*

Because of its sweeping nature, the CCPA is an unprecedented piece of legislation. By enshrining basic internet privacy rights, transferring essential control over consumer data back to consumers—rather than simply requiring transparency, as with CalOPPA—and placing the onus to enforce the law on state regulators rather than private citizens, California’s new law, broadly speaking, has much more in common with

177. *Id.* § 1798.150(b), amended by 2018 Cal. Legis. Serv. 735 (West).

178. *Id.* § 1798.155(b).

179. *Id.* § 1798.155(c)(1).

180. *Id.* § 1798.155(c)(2), amended by 2018 Cal. Legis. Serv. 735 (West).

181. *Id.* § 1798.185(a).

182. *Id.* § 1798.185(b).

GDPR than with other American privacy laws.¹⁸³ But does it also suggest a more “European” future for privacy law in the United States?

As discussed in Section I of this article, the answer is “in some cases, yes, in others, no.” While the CCPA may likely be a model—or at least a reference point—for future federal privacy legislation or similar copy-cat laws in other states,¹⁸⁴ underlying norms and values are not as easy to change. And regardless of whether the legislation will be a model for future statutes, it will likely emerge as the *de facto* national standard given the size and reach of California’s economy.¹⁸⁵ Europe has

183. See Sarah Meyer, *Tech Companies Ready to Battle New California Data Privacy Law*, CPO MAG. (July 13, 2018), <https://www.cpomagazine.com/2018/07/13/tech-companies-ready-to-battle-new-california-data-privacy-law/> (“The legislation bears a striking resemblance to the European Union General Data Protection Regulation (GDPR) and places responsibility for data use squarely in the hands of the consumer.”); Proskauer Summary, *supra* note 17 (“[I]t’s likely that many companies will find the compliance process as much of a struggle as their GDPR compliance efforts.”); Lydia de la Torre, *GDPR Matchup: The California Consumer Privacy Act 2018*, IAPP (July 31, 2018), <https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/> (“As the first U.S. attempt at a comprehensive data protection law, the CCPA has the potential to become as consequential as the GDPR. After all, California is the fifth largest economy in the world, the home of many technology titans, and traditionally a trend-setting state for data protection and privacy in the U.S.”); *California Moves Towards GDPR-Like Privacy Protections in the California Consumer Privacy Act of 2018*, FOLEY & LARDNER LLP (July 2, 2018), <https://www.foley.com/california-moves-towards-gdpr-like-privacy-protections-in-the-california-consumer-privacy-act-of-2018-07-02-2018/> (“The new law gives consumers broad rights to access and control of their personal information and imposes technical, notice, and financial obligations on affected businesses. CCPA was enacted to protect the privacy of California consumers and has some similar characteristics to the EU’s General Data Protection Regulation (GDPR), including a new and very broad definition of what is included in protected personal information.”). But see Tim Peterson, *Why California’s New Consumer Privacy Law Won’t Be GDPR 2.0*, DIGIDAY (July 9, 2018), <https://digiday.com/marketing/californias-consumer-privacy-law-has-digital-ad-industry-searching-for-answers/> (“The law does not prevent companies from collecting people’s information or give people an option to ask a company to stop collecting their information, differentiating it from GDPR.”).

184. Malcolm Chisholm, *California Consumer Privacy Act of 2018 v. GDPR*, FIRST S.F. PARTNERS (June 29, 2018), <https://www.firstsanfranciscopartners.com/blog/california-consumer-privacy-act-of-2018-vs-gdpr/> (“California often leads in innovations, and we can expect other states, and possibly the Federal government, to follow this initiative.”).

185. See Alex Gray, *Which American State Has a Bigger Economy Than India?*, WORLD ECON. FORUM (July 8, 2016), <https://www.weforum.org/agenda/2016/07/american-state-bigger-economy-than-india/> (“[I]f California were inserted into the world ranking by GDP according to country, it would come sixth—ahead of France, India, Italy and Brazil.”). See also Reece Hirsch and Kristin Hadgis, *INSIGHT: California’s New, GDPR-Like Privacy Law Is a Game-Changer*, BLOOMBERG BNA (July 11, 2018), <https://www.bna.com/insight-californias-new-n73014477375/> (“Whatever the CCPA’s national influence on lawmakers, for many companies it will be adopted as a *de facto* national standard.”); *California’s GDPR? Sweeping California Privacy Ballot Initiative Could Bring Sea Change to U.S. Privacy Regulation and Enforcement*, SIDLEY AUSTIN: PRIVACY AND CYBERSECURITY UPDATE (June 25, 2018), <https://www.sidley.com/en/insights/newsupdates/2018/06/sweeping-california-privacy-ballot-initiative-could-bring-sea-change>

historically considered the individual right to privacy as a value in and of itself, and has enshrined it explicitly in the ECPHR.¹⁸⁶ On the other hand, the free flow of information and its benefit to free enterprise has historically been much more significant in the U.S.¹⁸⁷ Also critical to the future of privacy legislation in the U.S., and perhaps as a result of these differences in values, the biggest tech companies tend to be American.¹⁸⁸ Despite nascent scrutiny of its practices in recent months, the tech community is likely—as it has in the past—to have considerable influence over future legal developments in the U.S., including amendments to the CCPA between now and 2020.¹⁸⁹

Assuming that U.S. tech companies will have tremendous influence over the drafting of future privacy legislation—whether at the state or federal level—arguably suggests that any future privacy regime on this side of the Atlantic will be much more favorable to those tech companies than the European regime. It will, in other words, continue to perpetuate the underlying, un-European values that helped Silicon Valley to flourish in the first place. However, there are also good reasons for tech companies, and other companies that traffic in personal information, to favor overarching federal internet privacy legislation. For example, there is always the incentive—once consumers’ and their legislators’ appetite for legislation has reached a tipping point—for business interests to get out in front of a movement and make concessions.¹⁹⁰ More importantly,

(“This initiative would likely create a de facto national standard on transparency around third-party sharing as well as consumer rights to restrict data sharing and could affect many business models that depend on data monetization to offer a free good or service.”).

186. See ECPHR, *supra* note 89.

187. See Monahan, *supra* note 85.

188. Kristin Stoller, *The World’s Largest Tech Companies 2018: Apple, Samsung Take Top Spots Again*, FORBES (June 6, 2018), <https://www.forbes.com/sites/kristinstoller/2018/06/06/worlds-largest-tech-companies-2018-global-2000/#41c38c244de6> (“Though the U.S. remains on top, Asian companies are slowly inching their way onto our list of the top technology companies in the world.”).

189. See David Meyer, ‘We Look Forward to Improvements.’ *Big Tech Plans to Fight Back Against California’s Sweeping New Data Privacy Law*, FORTUNE (July 2, 2018), <http://fortune.com/2018/07/02/california-data-privacy-ab-375-big-tech-fightback/> (quoting Google spokeswoman Katherine Williams: “We appreciate that California legislators recognize these issues and we look forward to improvements to address the many unintended consequences of the law.”); McKinnon & Vartabedian, *supra* note 12 (“The effort by tech coalitions . . . comes after the industry has fended off many types of federal action on privacy for years.”); Meyer, *supra* note 183 (“The battle lines have been drawn in the war for privacy protection. The ballot initiative seems to be off the table for now and tech companies are lobbying strongly to protect their right to use and sell data to thirds parties.”).

190. Indeed, according to a recent report in The New York Times, tech companies are already lobbying federal legislators for a more favorable law which would “overrule” the CCPA. Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), <https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html>

any federal legislation preempting state law, and potentially even supplanting portions of other federal laws such as HIPAA or GLBA, could greatly simplify the complex privacy regime discussed in this Article and thus reduce compliance costs for companies.¹⁹¹

It is also worth noting that, in addition to their lobbying advantage, big tech companies are best able—as incumbents, and given their massive financial resources—to comply with privacy legislation and regulations.¹⁹² In other words, sweeping privacy legislation and attendant regulations are likely, as any new legal regime, to hit medium- and small-sized companies hardest.¹⁹³

For now, at least, all U.S. companies will have to continue to navigate a complex and duplicative privacy regime, with overlap of laws governing different, narrower aspects of privacy as well as laws at the federal and state levels. Following enactment of the CCPA, the American regime may become an even more complex hybrid system: at once a uniquely American legal “Wild West,” where private citizens and the plaintiff’s bar enforce and sometimes abuse a number of key privacy laws, but also a European-style state regulatory Leviathan, with the Federal Trade Commission as the *de facto* privacy regulator and the California state attorney general moving into a similar role once the CCPA takes effect.¹⁹⁴

B. Suggestions for Moving Forward

Because the text of the CCPA does *not* place any restrictions on how it may be amended, there are, as a number of observers have pointed out, likely to be a number of changes to the law between now and when it goes into effect in 2020.¹⁹⁵ Below are some suggestions that would make

(“In recent months, Facebook, Google, IBM, Microsoft and others have aggressively lobbied officials in the Trump administration and elsewhere to start outlining a federal privacy law, according to administration officials and the companies. The law would have a dual purpose, they said: It would overrule the California law and instead put into place a kinder set of rules that would give the companies wide leeway over how personal digital information was handled.”).

191. *Id.* (“Top lobbyists for other tech companies agreed that [the CCPA] could be more problematic than the new European law, and that it would unleash a patchwork of state laws that would not only strap their businesses but become a regulatory headache, the people briefed on the meeting said.”).

192. Chris Wilson, *The GOP Needs a Free Facebook*, WALL ST. J. (Apr. 9, 2018), <https://www.wsj.com/articles/the-gop-needs-a-free-facebook-1523315383>.

193. Michael Hendrix, *Regulations Impact Small Business and the Heart of America’s Economy*, U.S. CHAMBER OF COMMERCE FOUND. (Mar. 14, 2017), <https://www.uschamberfoundation.org/blog/post/regulations-impact-small-business-and-heart-americas-economy>.

194. See Montezuma, *supra* note 22.

195. See, e.g., *Proskauer Summary*, *supra* note 17; Adam Schwartz et al., *How to Improve the California Consumer Privacy Act of 2018*, ELEC. FRONTIER FOUND. (Aug. 8, 2018), <https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018>;

the CCPA—and U.S. internet privacy law in general—clearer, fairer, and more effective.¹⁹⁶

1. Make the Private Right of Action More Meaningful

As the law is currently drafted, the California attorney general is in the driver's seat in terms of how the law is enforced. For that reason, much remains to be seen in terms of the impact the law will have on businesses. That said, because the law as it was passed removes the whistleblower provision¹⁹⁷ and the broad private right of action contained in the original ballot initiative, the attorney general is likely left with an impossible task: policing as many as a half million American businesses.¹⁹⁸

Sue Poremba, *Tech Companies Cool Toward California Consumer Privacy Act*, SECURITY BOULEVARD (July 24, 2018), <https://securityboulevard.com/2018/07/tech-companies-cool-toward-california-consumer-privacy-act/> (“Tech companies are expected to fight for changes before the law goes into effect. The bill was pushed through too quickly, they say, and it is too vague.”).

196. At least one bill, S.B. 1121, has already been introduced to amend the CCPA. The bill is relatively limited, and only purports to (1) except health care providers and covered entities from the law's purview; (2) “delete the requirement that a consumer bringing a private right of action notify the Attorney General”; and (3) limit civil penalties to be assessed by the Attorney General to not more than \$2,500 per violation or \$7,500 for intentional violations, rather than a \$7,500 limit for all violations. See S.B. 1121, 2017–18 Leg. Sess. (Cal. 2018), https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

197. See discussion *infra* Section IV.B.2.

198. See Heimes, *supra* note 139. In addition to specific adjustments to the CCPA text, the California legislature should take the opportunity to introduce meaningful cy pres reform. This practice has been particularly critical (and especially controversial) in the privacy context, with a number of high-profile privacy advocacy groups receiving large amounts of funding from privacy litigation. See Sara Randazzo, *Google Privacy Case Risks Disrupting a Key Source of Nonprofit Funding*, WALL ST. J. (Mar. 23, 2018), <https://www.wsj.com/articles/google-privacy-case-risks-disrupting-a-key-source-of-nonprofit-funding-1521797400>. In particular, the legislature should craft a regime in which awards from privacy litigation go only to (1) plaintiffs, (2) whistleblowers, and (3) the Consumer Privacy Fund already created by the CCPA. See Ted Frank, *Cy Pres Settlements*, ABA, https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2016_sac/written_materials/6_cy-pres_settlement.authcheckdam.pdf (summarizing the cy pres doctrine).

Authors have also discussed the constitutionality of the cy pres doctrine. See Jonah M. Knobler & Sam A. Yospe, *Frank v. Gaos: Cy Pres Gets Its Day at the Supreme Court*, 19 BLOOMBERG L. CLASS ACTION LITIG. REP. 587, 587–88 (2018), <https://www.pbwt.com/content/uploads/2018/06/KnoblerYospePublisCLASS1.pdf>. (“Increasingly, courts presiding over class actions employ a controversial practice called cy pres . . . that diverts damages owed to injured class members to non-party charitable institutions. The theory behind cy pres is that, when getting damage awards to class members is difficult, giving that money to a relevant charity is the next-best result. . . . Rule 23, which governs class actions in federal court, says nothing about cy pres. No statute affirmatively authorizes it. The Supreme Court has never said a word about it. . . . Some argue that cy pres is affirmatively prohibited by the Rules Enabling Act, the statute under which

In order for the CCPA to have its intended effect, it may be advisable to make the private right of action more meaningful by allowing citizens to sue in response to violations other than data breaches. The ballot initiative included a private right of action for injured consumers, including statutory damages of \$1,000 per violation and up to \$3,000 per violation for willful violations.¹⁹⁹ Although legislators should be careful about creating a “cash cow” situation for the plaintiff’s bar, a private right of action—perhaps with reduced statutory damages figures—would deputize a host of “private attorneys general,” allowing the private sector to better police itself. Provided the amount of litigation and dollar amounts are reasonable, allowing private lawsuits—and thus allowing courts to interpret and flesh out the CCPA’s various ambiguities—could also help provide clarity for the business community.²⁰⁰

2. Include a Whistleblower Provision

The ballot initiative originally included a whistleblower provision which would have helped deputize watchdogs to ensure compliance. Specifically, the ballot initiative provided that:

Any person who becomes aware, based on non-public information, that a person or business has violated this Act may file a civil action for civil penalties pursuant to [the Attorney General enforcement section], if prior to filing such action, the person files with the Attorney General a

the Federal Rules of Civil Procedure were promulgated. The Act states that those Rules—including Rule 23—“shall not abridge, enlarge or modify any substantive right.” 28 U.S.C. § 2072(b). . . . Indeed, some go even further and argue that class-action cy pres is unconstitutional. . . . For example, Article III’s ‘case or controversy’ requirement may prohibit federal courts from ordering monetary awards to non-parties that are strangers to an adversarial proceeding and lack an injury-in-fact traceable to the defendant.”) (citation omitted).

199. *Ballot Initiative*, *supra* note 132, at 13.

200. Unfortunately, the amendment process is not headed that direction. See Paul Karlsgodt, *California Consumer Privacy Act: Navigating Consumer Lawsuits & Limiting Remedies*, BAKER HOSTETLER: DATA PRIVACY MONITOR (Aug. 29, 2018), <https://www.dataprivacymonitor.com/state-legislation/california-consumer-privacy-act-navigating-consumer-lawsuits-limiting-remedies/> (“The CCPA was amended on June 25 to add subsection (c) of Section 1798.150 to clarify ‘Nothing in this act [proposed to be amended from “act” to “title”] shall be interpreted to serve as the basis for a private right of action under any other law.’ Based on this amendment, it appears that the California Legislature intends to preclude having a business’s violation of the CCPA serve as a basis for a claim under California’s Unfair Competition Law (UCL), California Business and Professions Code (BPC) §§ 17200 et seq., which permits a private right of action for claims based on unlawful, unfair, or fraudulent business acts or practices—or under ‘any other law.’”).

written request for the Attorney General to commence the action.²⁰¹

Any whistleblower whose civil suit resulted in penalties would have been entitled to “an amount the court determines is reasonable,” but “not less than 25 percent and not more than 50 percent of the proceeds of the action.”²⁰²

A similar provision in the CCPA may help the law achieve its stated ends. In reality, the attorney general simply does not have the capacity to police a half million U.S. businesses. Putting the same or a substantially similar whistleblower provision—such as those in Sarbanes-Oxley and Dodd-Frank, for example—back into the legislation would likely result in more effective and more efficient enforcement; requiring whistleblowers to filter their claims through the attorney general could do so without unleashing a tidal wave of frivolous lawsuits.

3. Implement a More Effective Cure Period

The CCPA’s thirty-day cure period is also problematic, but from two opposite perspectives. For relatively small or simple violations, a cure period arguably renders the enforcement provisions toothless—businesses will simply fix these types of problems as they surface rather than being proactive and compliant on the front-end. But a thirty-day cure period may be far too short for larger, more complex violations, as company-wide corrections would typically take much longer than this.

If the final version of the CCPA includes a cure period, it may make sense for it to be extended. This would not affect simple violations, which could likely be cured in thirty days, but would allow for systemic problems to be properly addressed and rectified, thus giving the provision meaning. Alternatively, the legislature could institute separate cure periods based on the nature of the violation.

4. Clarify the Definition of “Publicly Available” Information

As discussed above, the CCPA excludes “publicly available information” from the definition of personal information.²⁰³ Publicly available information is defined as “information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information.”²⁰⁴ The law also provides that:

201. *Ballot Initiative*, *supra* note 132, at 15.

202. *Id.* at 16.

203. CAL. CIV. CODE § 1798.140(o)(2) (West 2018).

204. *Id.*

“Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge. Information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. “Publicly available” does not include consumer information that is deidentified or aggregate consumer information.²⁰⁵

Despite these additional clarifications, the statute’s definition remains vague. Most importantly, the inquiry into whether the purposes of the information’s use and the original purposes for which it is maintained are “compatible” may raise a host of arguable questions about how personal information is being used. In the absence of further guidance in the statute, courts and regulators will likely have to drill down and ask questions about the original intent and purpose of statutes governing publicly available information in government records in order to determine whether subsequent uses are “compatible with the purpose for which the data is maintained.” Likewise, there may be arguments around what constitutes “aggregate” consumer information.

5. Clarify the Deletion Requirement

As discussed above, Section 1798.105 allows a consumer to “request that a business delete any personal information about the consumer which the business has collected from the consumer.”²⁰⁶ But this deletion requirement potentially raises as many questions as it answers. Does the information have to be deleted forever? What if the information is later reobtained in some other, lawful way? The Act also requires businesses that receive a deletion request to also “direct any service providers to delete the consumer’s personal information.”²⁰⁷ But what if the service provider refuses or is unable to comply? And how, in any case, would the covered business verify the service provider’s compliance? Will the covered business be directly liable for any acts or omissions of the service provider? The structure contemplated here may result in a contractual flow similar to the GDPR data protection agreements and standard contractual clauses arising out of the data processor–data controller relationships.²⁰⁸

205. *Id.*

206. *Id.* § 1798.105(a).

207. *Id.* § 1798.105(c).

208. For an overview of data protection agreements between controllers and processors and standard contractual clauses, see *New Standard Contractual Clauses for Data Transfers Out of*

Additionally, the deletion requirement contains a number of exceptions, which are open to interpretation. For example, the business is not required to comply with the request if it is necessary to maintain the personal information in order to “provide a good or service requested by the consumer.”²⁰⁹ Does this inherently require businesses to respond to a deletion request by informing consumers how deletion of their data might affect services they are receiving, or are businesses allowed to simply ignore the request unless the consumer expressly requests deletion *even if it means canceling his or her services*? This section also allows business to maintain personal information in order to “[e]xercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise *another right provided for by law*.”²¹⁰ What rights are included in this last, catch-all language? The right to perform contract obligations to a third party?

This section also allows businesses to maintain personal information “[t]o enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business”²¹¹ or to “use the consumer’s personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.”²¹² As with the “publicly available information” definition, the CCPA’s reference to “the expectations of the consumer,” not defined, introduces needless ambiguity into the statute and should be cleaned from the law. Although businesses of course have an idea of consumer expectations in certain kinds of simple cases—a consumer who gives her phone number to a delivery company would expect her number be given to the delivery man in case the delivery man cannot find her house, for example—but there are likely to be a number of situations where “consumer expectations” will be complex and impossible for businesses to divine. Likewise, the allowance for internal uses that are “compatible with the context in which the consumer provided the information” raises similar questions about the meaning of “compatibility” discussed above.

6. Clarify the Interplay with Federal Statutes

As discussed above, the CCPA exempts certain personal information that is also covered by HIPAA, the GLBA, the FCRA, and the DPPA.²¹³

the European Union Raise Concerns, JONES DAY (July 2010), https://www.jonesday.com/new_standard_contractual_clauses/.

209. CAL. CIV. CODE § 1798.105(d)(1).

210. *Id.* § 1798.105(d)(4) (emphasis added).

211. *Id.* § 1798.105(d)(7).

212. *Id.* § 1798.105(d)(9).

213. *Id.* § 1798.145(c)–(f).

But these exemptions are, as with other key terms in the Act, plagued by ambiguities. For example, in the case of HIPAA, the statute says that it “shall not apply to . . . protected health information that is collected by a covered entity.”²¹⁴ But what about information collected *on behalf* of a covered entity? Does the exclusion apply to business associates, as a general matter?²¹⁵

In the cases of overlaps with the GLBA and DPPA, what constitutes a conflict between these two laws and the CCPA that would trigger an exclusion? Must the conflict be direct? What about additional terms present in one statute but not another? Does the fact that the CCPA includes statutory damages but the GLBA does not constitute a conflict? And how do the provisions excluding GLBA- and DPPA-covered information in the case of a conflict interplay with Section 1798.175 of the CCPA, which states that “in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.”²¹⁶ Does this mean that in cases where there is a conflict between the Act and the relevant federal statute, the CCPA may nevertheless apply if it is deemed to afford greater privacy protections?

There are even more fundamental questions about interplay with federal statutes. Why have a full exemption for personal information covered by HIPAA and the FCRA, but only this qualified exemption for the GLBA and DPPA? And why choose these four laws over other privacy laws in the first place?

214. *Id.* § 1798.145(c)(1)(A). Under HIPAA, a “covered entity” is defined as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards, and may include a business associate of another covered entity. 45 C.F.R. § 160.103 (2019); see *Who Must Comply with HIPAA Privacy Standards?*, U.S. DEP’T. OF HEALTH & HUMAN SERVS., <https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html> (last updated July 26, 2013).

215. A “business associate” is “a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.” *Business Associates*, U.S. DEPT. OF HEALTH & HUMAN SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html> (last updated July 26, 2013); see Adam H. Greene, *How a Rushed California Law Will Change the Privacy and Security Landscape for Mobile Health Apps*, LEXOLOGY (July 27, 2018), <https://www.lexology.com/library/detail.aspx?g=06756c7a-61a5-4230-8505-7e2f26baa169> (“It is unclear whether the law will apply to protected health information of mobile health app developers who are business associates under HIPAA.”).

216. CAL. CIV. CODE § 1798.175.

7. Clarify the 12-Month Requirement

The legislature should also amend the CCPA to clarify that requirements to disclose what personal information has been collected, sold, or disclosed for a business purpose in the “preceding 12 months” is not a running requirement, but rather a requirement to update such information once each calendar year.²¹⁷ As currently crafted, it is not at all clear whether this is an annual requirement, or a requirement that businesses constantly update this 12-month “lookback” so that it is always accurate. The latter would be unreasonable. Consider, for example, a situation where a market research firm enters into an agreement with a panel company, pursuant to which the panel company provides the market research firm with access to panels for survey research purposes. Does the CCPA require the market research firm to check in with the panel company (and any other panel companies it has engaged) every day to make sure the panel company is not collecting new categories of personal information from panel members? Is the panel company required to keep a running tab of what information its myriad clients are collecting from its panel members?

The reality is that many businesses, even small- and medium-sized businesses, have relationships and data sets that are often highly dynamic. They may have several agreements, pursuant to which they may share large quantities of personal information. Additionally, they may collect personal information from other businesses that are not parties to the agreements. These factors require businesses to offer individuals an accurate 12-month snapshot of what it is doing with personal information. Accordingly, the legislature should clarify that the 12-month requirement is an *annual* requirement to update its disclosures.

8. Expand the Carve-Out for “Research”

As discussed above, the Act exempts from the deletion requirement businesses engaged in “public or peer-reviewed scientific, historical, or statistical research . . . when the businesses’ deletion of the information is likely to render impossible or seriously impair the achievement of such research . . .”²¹⁸ Elsewhere in the Act, “research” is defined as “scientific, systematic study and observation, including basic research or applied

217. The phrase “preceding 12 months” appears a number of places in Section 1798.130, which among other things requires businesses to: “Identify by category or categories the personal information collected about the consumer in the preceding 12 months”; “[i]dentify by category or categories the personal information of the consumer that the business sold in the preceding 12 months”; and “[i]dentify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months.” *Id.* § 1798.130(a)(3)(B), (a)(4)(B)–(C).

218. *Id.* § 1798.105(d)(6).

research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health.”²¹⁹

As currently drafted, this exception appears to be very narrow, applying only to non-profit or academic research. The research definition should be expanded to include for-profit research. It is not only academic researchers who deal in personal information without the end goal of direct marketing and sales to consumers.²²⁰ For-profit market research firms also play a critical role in helping ensure healthy relationships between businesses and consumers, doctors and patients, and politicians and constituents by helping for-profit and non-profit businesses, as well as governmental entities, better understand the public.²²¹ This distinction between direct sales and marketing on one hand, and research—including for-profit research—on the other, is well established in the privacy context. The FTC’s Telemarketing Sales Rule, for example, forbids “sales under the guise of research,” or “sugging,” a ban for which the market research industry actively lobbied.²²² Likewise, the FCC has for decades drawn this distinction in its TCPA rules.²²³

Furthermore, because the research carve-out only applies to the deletion requirement, it fails to adequately protect research from the burdens of the CCPA. Because the CCPA—as are a number of other internet privacy laws—is focused on more directly commercial uses of personal information, a broader exemption for research, like that in place

219. *Id.* § 1798.140(s).

220. The Insights Association, the largest trade association for the market research industry, binds its members to an ethics code which forbids members from advertising and direct marketing based on a respondent’s participation in research. See *Insights Association Code of Standards and Ethics for Marketing Research and Data Analytics*, INSIGHTS ASS’N (May 10, 2018), <https://www.insightsassociation.org/issues-policies/insights-association-code-standards-and-ethics-market-research-and-data-analytics-0> (“When engaging in non-research activities (for example, promotional or commercial activities directed at data subjects, including but not limited to advertising and direct marketing), do not permit any direct action to be taken against an individual based on his or her participation in research.”).

221. See *id.*

222. Telemarketing Sales Rule, 16 C.F.R. § 310 *et seq.* See Diane K. Bowers, *Sugging Banned at Last*, MKTG. RESEARCH, Fall 1995, at 40 (“With support from the Direct Marketing Association and the National Association of Attorneys General, the Council for Marketing and Opinion Research (CMOR) succeeded in having an amendment approved to prevent ‘sugging’ (selling under the guise of research).”).

223. See, e.g., Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 7 FCC Rcd. 8752 ¶ 41 (1992) (“[T]he exemption for non-commercial calls from the prohibition on prerecorded messages to residences includes calls conducting research, [or] market surveys . . . ”); Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991, Report and Order, 27 FCC Rcd. 1830 ¶ 28 (2012) (explaining that “research or survey calls” made with an autodialer to residential wireline consumers do not require consent if they do not contain telemarketing messages).

in the TCPA context, would better protect the valuable role researchers play in the marketplace without hampering the law's broader objectives.

9. Streamline the Disclosure Requirements

Finally, the legislature should streamline the requirements around what must be disclosed to consumers regarding the collection, sale, and use of their personal information. As discussed above, Section 1798.130 requires businesses to disclose a host of information in its online privacy policies, including: a description of a consumer's rights; categories of personal information collected; categories of sources from which personal information has been collected; business or commercial purposes for collection or sale; categories of personal information sold or disclosed for a business purpose; the right to opt out of the sale of personal information; and the consumer's right to request deletion of personal information.²²⁴ In addition, under Section 1798.110, businesses that collect the personal information must also disclose the specific pieces of personal information collected.²²⁵

There are a handful of problems with these disclosure requirements as presently drafted. First, the statute offers very limited guidance on what might constitute "categories" of personal information or sources of personal information collected²²⁶: information and sources of information could theoretically be grouped in any number of ways. Because the costs to businesses of comprehensive audits of their data practices for the purpose of defining these categories are likely to outweigh the benefits, the Act should instead impose a more comprehensive, general requirement that a business disclose the nature of its business as it relates to the collection of personal information.

Second, requiring businesses to disclose with any specificity the business or commercial purposes of their data collection and use practices may cross a line by requiring businesses to disclose closely held strategic information or even trade secrets. Here, too, substituting a broader requirement that businesses explain the nature of their business models in more general terms would serve the Act's purposes.

Third, instead of including an open-ended requirement that businesses disclose all the "specific pieces" of personal information collected if

224. CAL. CIV. CODE § 1798.130(a)(5).

225. *Id.* § 1798.110(a)(5), (c)(5).

226. The only guidance offered is found in the Act's introductory section: "Many businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories." *Id.* § 1798.100(e), *amended by* 2018 Cal. Legis. Serv. 735 (West).

requested by an individual, the Act should set a list of pieces of information which must be disclosed. This could be accomplished efficiently by using the personal information examples included in Section 1798.140(o)(1) as a checklist. Further, the list of examples in this section could be an exclusive list, which would remove ambiguity around what specific pieces of information should be disclosed to the individual, as well as clarify the personal information definition.²²⁷

Finally, legislators should delete the requirement that privacy policies include a “description of a consumer’s rights pursuant to Sections 1798.110, 1798.115, and 1798.125.”²²⁸ Statistics show that consumers already actually bother to read privacy policies at a dismally low rate.²²⁹ Requiring companies to explain to consumers multiple provisions of a complex statute, in addition to disclosures that are already specific to other laws like GDPR, will only undermine the purpose of privacy policies in the first place: that users read and understand how a business is collecting, using, and sharing or selling their information.

CONCLUSION

While it has taken some time for consumers to apprehend the full scope and nature of Web 2.0, there seems to be a new appetite among consumers and legislators alike for broad, sweeping privacy legislation. Certainly, there are already a large number of privacy laws on the books, but these have largely been aimed at specific, ascertainably urgent and easier-to-understand problems such as data breach notification, protection of sensitive health and financial information, or children’s privacy.²³⁰

In contrast with America, Europe has relied less on plaintiffs’ lawyers and private attorneys general, and more on centralized regulators—most notably through GDPR, passed earlier this year.²³¹ Is sweeping legislation in the mold of GDPR around the corner in America?²³² Maybe, maybe

227. See *id.* § 1798.140(o)(1) (“Personal information includes, but is not limited to, the following . . .”). A reasonable amendment might be to delete the phrase “but is not limited to” from this section.

228. *Id.* § 1798.130(a)(5)(A).

229. See sources cited *supra* note 1; Florian Schaub, *Nobody Reads Privacy Policies—Here’s How to Fix That*, SALON (Oct. 14, 2017), https://www.salon.com/2017/10/14/nobody-reads-privacy-policies-heres-how-to-fix-that_partner/ (“In 2008 a study estimated that it would take 244 hours a year for the typical American internet user to read the privacy policies of all websites he or she visits . . .”).

230. See *supra* Part II.

231. See *supra* Part III.

232. See, e.g., Cameron F. Kerry, *Filling the Gaps in U.S. Data Privacy Laws*, BROOKINGS INST. (July 12, 2018), <https://www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws/> (“The Cambridge Analytica stories, the Mark Zuckerberg hearings, and

not. But if so, the CCPA will likely be at the center of this development, both as a potential model for federal legislation or copy-cat laws in other states, and even as a de facto national privacy law when it goes into effect in 2020. Broadly, the CCPA grants consumers four basic rights in connection to their personal data: (1) the right to know what personal information is collected; (2) the right to “opt-out” of a business selling their personal information; (3) the right to have a business delete their personal information; and (4) the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.²³³ These rights are largely to be enforced by the California Attorney General, with a narrow private right of action for data breaches.²³⁴

Although the bill will likely be amended before it goes into effect in 2020, the final law is almost certain, in light of the size and reach of the California economy, to be a game changer for U.S. privacy law. A number of amendments would make the law clearer and fairer, both to businesses and individual data subjects, including: making the private right of action more meaningful; a whistleblower provision to make take some of the enforcement burden off the attorney general; implementing a more effective cure period; clarifying the definition of “publicly available” information, the deletion requirement, the statute’s interplay with federal statutes, and the 12-month notification requirement; expanding the carve-out for research; and streamlining the disclosure requirements.

the constant reports of major data breaches have increased interest in federal privacy legislation. Various groupings have been convening to develop proposals. The time is ripe for interests to converge on comprehensive federal privacy legislation.”).

233. *Proskauer Summary*, *supra* note 17.

234. *See supra* Section IV.B.5.

BENEFIT OF THE BUT-FOR BARGAIN: ASSESSING ECONOMIC TOOLS FOR DATA PRIVACY LITIGATION

*Mike Kheyfets**

I.	INTRODUCTION	115
II.	ECONOMIC FRAMEWORK IN DATA BREACH CLASS ACTIONS AND POTENTIAL RELEVANCE OF “CONJOINT ANALYSIS”	116
III.	“HOLD THE PICKLES, HOLD THE . . . ADEQUATE AND REASONABLE DATA SECURITY”: CAN CONJOINT ANALYSIS IDENTIFY THE “BARGAIN” ON THE RELEVANT FEATURE?.....	120
IV.	“P-R-I-V-A-C-Y IS PRICELESS TO ME”: CAN CONJOINT ANALYSIS IDENTIFY AN ECONOMICALLY OBJECTIVE VALUE OF THE RELEVANT FEATURE?	123
V.	“ALL FOR ONE AND ONE FOR ALL”: CAN CONJOINT ANALYSIS BE USED TO SHOW A BREACH’S IMPACT ON ALL (OR NEARLY ALL) PROPOSED CLASS MEMBERS?	131

I. INTRODUCTION

A theory of harm frequently asserted in data breach class actions is that plaintiffs did not receive the “benefit of the bargain” with defendants. That is, plaintiffs claim that when they transferred sensitive information to defendants, they anticipated that the information would remain safe. When the data were exposed as part of a breach, that “bargain” was not upheld. For example, *Anthem* plaintiffs alleged that when purchasing health insurance, they suffered “loss of the benefit of the bargain with Defendants to provide *adequate and reasonable data security*” and instead received health insurance that was “less valuable than described in their contracts.”¹ Similar theories have been alleged in a variety of data privacy class actions.² For example, in retail breach cases: (i) *P.F.*

* Partner in the Antitrust and Privacy & Data Security practices at Edgeworth Economics, L.L.C. I would like to thank Jesse David, Mike Will, and Adam Cooke for their helpful feedback.

1. Fourth Consolidated Amended Class Action Complaint at 120, 135, *In re Anthem Data Breach Litig.*, No. 15-MD-02617-LHK (N.D. Cal. Feb. 24, 2017), ECF No. 714-3 [hereinafter *Anthem Complaint*] (emphasis added).

2. See, e.g., *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012) (alleging that portions of plaintiffs’ insurance premiums were consideration for an insurer’s promises to provide data

Chang's plaintiffs claimed damages on "the cost of their meals" because they "would not have dined at P.F. Chang's had they known of its poor data security,"³ and (ii) *Neiman Marcus* plaintiffs argued they overpaid because "the store failed to invest in an adequate security system."⁴

Methods to analyze benefit of the bargain harm in a class certification setting have continued to evolve. For example, while *P.F. Chang's* and *Neiman Marcus* plaintiffs did not propose any specific analytical framework for assessing this theory, *Anthem* plaintiffs suggested that they would use a statistical technique called "conjoint analysis" to do so.⁵

II. ECONOMIC FRAMEWORK IN DATA BREACH CLASS ACTIONS AND POTENTIAL RELEVANCE OF "CONJOINT ANALYSIS"

"The appropriateness of the class action mechanism for adjudicating a consumer data breach litigation rests crucially on the plaintiffs' ability to present an analysis capable of determining whether all—or, in some cases, virtually all—class members could have suffered injury from the alleged data breach," as well as the estimation of damages on a class-wide

security); *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-MD-2586, 2016 WL 81792 (D. Minn. Jan. 7, 2016) (alleging a variety of standing theories, including lost benefit of bargain); *In re LinkedIn User Privacy Litig.*, 309 F.R.D. 573 (N.D. Cal. 2015) (claiming plaintiff purchased her premium subscription on the basis of LinkedIn's statement that its users' data will be secured in accordance with industry standards); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015) (alleging to have signed a contract with Google indicating plaintiff was to receive a payment processing service that would facilitate her app purchase while keeping her private information confidential); *In re Adobe Systems, Inc. Privacy Litig.*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014) (alleging plaintiffs personally spent more on the defendant's products than they would have, had they known the defendant was not providing the reasonable security it represented it was providing.); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8167, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) (asserting plaintiffs overpaid for the products and services purchased from Barnes & Noble because they were paying for the security measures Barnes & Noble was supposed to employ to protect credit and debit transaction information).

3. *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016).

4. *Remijas v. Neiman Marcus Group*, 794 F.3d 688, 694 (7th Cir. 2015). The way the specific "bargain" between plaintiffs and defendants is described varies from case to case. However, for consistency, this article refers to the feature at issue using *Anthem* plaintiffs' terminology: that they understood their purchases to include a feature called "adequate and reasonable data security." *Anthem Complaint*, *supra* note 1, at 120.

5. Notably, *Anthem* plaintiffs indicated that the conjoint analysis "could not be completed until after class certification" because "the parameters of the conjoint surveys would depend on the classes ultimately certified by the Court." Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement at 4, 16, *In re Anthem Data Breach Litig.*, No. 15-MD-02617-LHK (N.D. Cal. June 23, 2017), ECF No. 869-5.

basis.⁶ Moreover, because plaintiffs often allege multiple theories of economic harm,⁷ such an analysis should distinguish between the damages associated with the different theories.⁸

With respect to a benefit of the bargain theory, a consumer's damages may be measurable as the difference between what the consumer *actually paid* for a product (i.e., in the "actual world") and what the consumer *would have paid* (i.e., in the "but-for world")⁹ for a product that did not allegedly misrepresent its level of "adequate and reasonable data security." This difference is meant to represent the "benefit" a defendant allegedly failed to deliver to its customers. The actual price paid for a product may be observable from invoices, consumer receipts, or point-of-sale records. However, the question relevant to assessing impact and damages is: What price *would* the consumer have paid if the defendant appropriately described the bargain at the time of the transaction, i.e., that it did not include adequate and reasonable data security?

Conjoint analysis—the technique suggested by *Anthem* plaintiffs to assess this question—is a "popular marketing research technique that marketers use to determine what features a new product should have and

6. David Cohen, Michael Kheyfets, Michelle Visser, & Adam Winship, *A Rigorous Analysis of Class Certification Issues in Consumer Data Breach Litigation*, 16 *PRIVACY & SECURITY L. REP.* 104, 107 (2017).

7. *Id.*

8. For example, in instances where plaintiffs have alleged they were harmed due to (i) fraudulent misuse of the stolen information, as well as (ii) not receiving the benefit of the bargain, their class certification and damages frameworks should be able to distinguish between the two.

9. As the *Anthem* plaintiffs described it, they suffered:

[L]oss of the benefit of the bargain with Defendants to provide adequate and reasonable data security—i.e. the difference in value between *what Plaintiffs should have received from Defendants* when they enrolled in and/or purchased insurance from Defendants that Defendants represented, contractually and otherwise, would be protected by reasonable data security, and *Defendants' partial, defective, and deficient performance* by failing to provide reasonable and adequate data security and failing to protect Plaintiffs' Personal Information from theft."

Anthem Complaint, *supra* note 1, at 120–21 (emphasis added); see, e.g., Federal Judicial Center, *Reference Manual on Scientific Evidence* 432 (3d ed. 2011). Note that what the plaintiffs would have paid in the but-for world is not necessarily the same as what they would have been *willing* to pay. As I discuss in more detail below, consumer willingness to pay is just one part of how prices are set in the real world.

how it should be priced.”¹⁰ In practice, it is implemented by first conducting a survey which asks respondents to choose among a series of hypothetical products with a variety of prices and features.

Exhibit 1 illustrates a survey that breaks down a consumer’s choice of which TV to buy into “attributes” such as screen type, screen size, brand, and price. The consumer is also offered a choice of various combinations of attribute “levels.” By offering respondents different combinations of attributes (e.g., a 36" Plasma Sony TV for \$499 vs. a 46" LED Philips TV for \$899),¹¹ a well-designed conjoint survey aims to gather information that can be used to study their preferences for individual attributes.

EXHIBIT 1¹²

A typical “Choice task”

Which of these TVs would you choose?				
Type	Plasma	LCD	LED	
Size	36 inch	40 inch	46 inch	
Brand	Sony	Toshiba	Philips	
Price	\$499	\$699	\$899	
	☐	☐	☐	

“Attributes” Three “Product profiles”
each of four attributes

“Levels” for each attribute

Once choice data from these surveys are collected, the goal of the conjoint analysis is to statistically model the weight (called “utility” or “part-worth”) respondents place on a given feature—relative to the

10. Joseph Curry, *Data Use: Understanding Conjoint Analysis in 15 Minutes*, QUIRK’S MARKETING RES. REV. (1996), <https://www.sawtoothsoftware.com/download/techpap/undca15.pdf> [hereinafter Curry, *Understanding Conjoint Analysis*].

11. In some conjoint surveys, the respondent may be asked to rank the choices from most-to least-preferred. In others, the respondent may be asked to make a single selection from the available choices.

12. *Conjoint Analysis*, DOBNEY, http://www.dobney.com/Conjoint/Conjoint_analysis.htm (last visited Sept. 25, 2018).

products' other features—when making their choices.¹³ Moreover, the respondents' collective valuation (or “willingness to pay”) for a feature can be derived through a calculation involving the “utility” of that feature and the “utility” of price.¹⁴

Courts have accepted this technique in several patent infringement cases involving reasonable royalty damages, with the goal of using it to isolate the value of an allegedly infringing feature by (indirectly) comparing versions of a product with and without that feature.¹⁵ In these cases, experts have argued that such valuations would have been considered by the parties in a hypothetical negotiation for royalties.¹⁶ More recently, conjoint analysis has been offered in consumer product mislabeling class actions. In such cases, plaintiffs allege that a manufacturer of a consumer product made false or misleading claims, and aim to use conjoint analysis to estimate the value of the allegedly misrepresented feature (e.g., the value related to labeling a product as “All Natural,” as compared to one without that label).¹⁷

Whether courts will accept conjoint analysis to certify classes in data breach cases remains uncertain.¹⁸ This Article discusses several key features of conjoint analysis, as well as challenges for the use of such

13. Curry, *Understanding Conjoint Analysis*, *supra* note 10.

14. To use terminology from *Anthem*, the survey would seek to identify respondents' perceived valuation of—or willingness to pay for—adequate and reasonable data security. *Anthem Complaint*, *supra* note 1, at 120.

15. See generally *Apple, Inc. v. Samsung Elecs. Co.*, No. 11-CV-01846-LHK, 2013 U.S. Dist. LEXIS 149741 (N.D. Cal. Oct. 15, 2013); *Microsoft Corp. v. Motorola, Inc.*, No. C10-1823-JLR, 2011 U.S. Dist. LEXIS 73827 (W.D. Wash. May 31, 2011).

16. See cases cited *supra* note 15.

17. See, e.g., *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1123 (9th Cir. 2016) (arguing that the “100% Natural” label on the product was false or misleading because Wesson oils are made from bioengineered ingredients that plaintiffs contended were “not natural”); *In re Dial Complete Mktg. & Sales Practices Litig.*, 312 F.R.D. 36, 47 (D.N.H. 2015) (alleging that a variety of statements appearing on Dial Complete's product labels, including claims that it “Kills 99.99% of Germs,” is “#1 Doctor Recommended,” and “Kills more germs than any other liquid hand soap” were inaccurate and misleading); *In re NJOY, Inc. Consumer Class Action Litig.*, No. CV 14-00428 MMM (RZx), 2014 U.S. Dist. LEXIS 199368, at *6 (C.D. Cal. Oct. 20, 2014) (alleging that NJOY's failure to include certain harmful ingredients on the label was misleading because consumers would want to know that the product contained these ingredients before purchasing e-cigarettes and that NJOY failed to warn of the harmful effects of inhaling such ingredients).

18. For example, plaintiffs in *Anthem* indicated that “the Benefit of the Bargain theory depended upon the results of a conjoint study that *could not be completed until after class certification*, and there was no guarantee that Plaintiffs would ultimately have found this type of damage *at all*.” Plaintiffs' Memorandum in Support of Preliminary Approval of Class Action Settlement at 21, *In re Anthem Data Breach Litig.*, No. 15-MD-02617-LHK (N.D. Cal. Feb. 24, 2017), ECF No. 869-5 (emphasis added). Plaintiffs also indicated that “it is possible that both the Benefit of the Bargain theory and the Loss of Value of PII theory could yield large numbers that would be unpalatable to a jury.” *Id.*

analysis in the context of class certification issues in data breach litigation. Specifically, conjoint surveys may: (i) struggle to isolate the purported bargain at issue in a data breach case; (ii) aim to measure the customer's *willingness* to pay for something rather than the price that prevails in the marketplace; and (iii) not yield results that represent all, or nearly all, members of a proposed class.

III. "HOLD THE PICKLES, HOLD THE . . . ADEQUATE AND REASONABLE DATA SECURITY": CAN CONJOINT ANALYSIS IDENTIFY THE "BARGAIN" ON THE RELEVANT FEATURE?

Conjoint analysis does not study actual transactions where sensitive information is exchanged. Rather, it surveys individuals—who may or may not be party to a proposed class—on their preferences for certain products relative to others. At least some products in the respondent's "choice set" are *hypothetical* in that they lack a feature that is actually offered in the real-world marketplace. There are two initial issues relating to hypothetical products that merit consideration. First, hypothetical products necessarily have hypothetical features—or actual features in hypothetical combinations—and prices that are set by the survey designer. Thus, the choices about what combinations of features are offered in the hypothetical products, as well as the price points for those products, necessarily influence the outcome of the survey. More importantly, however—and perhaps where analysis in data breach cases begins to depart from that in patent infringement and false claims cases—is that it may be difficult to assess how the notion of adequate and reasonable data security figures into consumers' choices.

For conjoint analysis to serve its purpose, the attributes among which respondents are choosing must be ones that affect the purchase process. For example, consumers may have a relatively clear perception of how much more they would be willing to pay for a mobile phone with a touchscreen than for one without, or a food product with an "All Natural" label than a similar product without the label. However, consumers may have more difficulty with an abstract concept like adequate and reasonable data security, particularly since that feature is not typically advertised or described by sellers of consumer products and services.

A conjoint analysis seeking to assess a claim like the one in *Anthem*—i.e., that purchasers of health insurance were deprived of adequate data security—may face the issue in the real world that consumers do not explicitly consider data security. For example, one academic study identified ten "key drivers of consumer choice among health-care coverage alternatives" as: (i) carrier providing health care coverage; (ii) doctor quality; (iii) hospital choice; (iv) monthly premium; (v) physician network; (vi) cost per doctor visit; (vii) prescription coverage; (viii)

wellness visits coverage; (ix) dental coverage; and (x) vision coverage.¹⁹ Even this list, which goes beyond the six-attribute “choice sets” generally prescribed by conjoint analysis practitioners,²⁰ does not leave room to identify the feature at issue in a data breach litigation. It may be difficult to tease out respondents’ valuation of such a feature if, in a real-world setting, they would not consider purchasing the “but-for” version of the product. Moreover, unlike the binary choice between a product either having an “all-natural” label or not, “data security” may be open to the respondent’s interpretation, further compounding the problem.

An issue with applying conjoint analysis to a “tough-to-value” feature arose in *Sanchez-Knutson v. Ford Motor Co.*²¹ In that case, plaintiffs alleged that certain Ford Explorer vehicles were defective because they experienced exhaust odor under certain driving conditions.²² Plaintiffs’ expert opined that he could design a conjoint analysis that would enable him to “determine the difference in value . . . that customers place on a Ford Explorer with no exhaust leaking into the cabin compared to an otherwise identical Ford Explorer subject to the problems with exhaust.”²³ The court took issue with this approach, stating “I don’t know how you do that analysis when no one’s gonna buy a car if it fills up with carbon monoxide when you drive it,” and indicating that if “you ask a bunch of people, how much would you pay for a Ford Explorer that has carbon monoxide in it . . . they’re all going to say nothing.”²⁴

Asking survey respondents what they would be willing to pay for health insurance without adequate and reasonable data security may yield similar results. Plaintiffs’ expert in *Anthem* recognized that “a critical aspect of the survey will be to specify a set of levels for the data security attribute,” and hypothesized three formulations of the feature at issue²⁵:

19. Roger Gates et al., *Modeling Consumer Health Plan Choice Behavior to Improve Customer Value and Health Plan Market Share*, 48 J. BUS. RES. 247, 250 tbl.1 (2000).

20. Paul E. Green & V. Srinivasan, *Conjoint Analysis in Marketing: New Developments with Implications for Research and Practice*, 54 J. MARKETING 3, 8–9 (1990).

21. *Sanchez-Knutson v. Ford Motor Co.*, 52 F. Supp. 3d 1223 (2014).

22. *Id.* at 1225.

23. Defendant Ford Motor Company’s Motion *In Limine* to Exclude the Testimony of Steven Gaskin at 2, *Sanchez-Knutson v. Ford Motor Co.*, No. 0:14-CV-61344-WPD (S.D. Fla. 2017), ECF No. 182.

24. *Id.* at 17. Notably, the Court in this case certified part of the proposed class, despite Plaintiffs having not actually executed the conjoint analysis at the time of the decision (“[T]he Court disagrees with Defendant that [plaintiffs’ expert], must have already performed his proposed conjoint analysis for the Court to consider the proffered methodology.”). Order Granting in Part and Denying in Part Plaintiff’s Renewed Motion for Class Certification at 14, *Sanchez-Knutson v. Ford Motor Co.*, No. 0:14-CV-61344-WPD (S.D. Fla. 2017), ECF No. 148.

25. Expert Report of Peter E. Rossi, *In re Anthem Data Breach Litig.*, No. 15-MD-02617-LHK (N.D. Cal. Feb. 24, 2017), ECF No. 720-30 [hereinafter Rossi Report].

Example 1:

1. Highest Level: Exceeds industry standards.
2. Intermediate Level: Meets industry standards.
3. Lowest Level: Falls short of industry standards in one or more important areas.

Example 2:

1. Meets or exceeds industry average for 11 of 13 metrics used in standard security audits.
2. Meets or exceeds industry average for 8 of 13 metrics used in standard security audits.
3. Meets or exceeds industry average for 5 of 13 metrics used in standard security audits.

Example 3:

1. All fundamental data security practices are adhered to.
2. One or more fundamental data security practices is (sic) not adhered to.

Because *Anthem* plaintiffs did not ultimately conduct this survey, it remains unknown which, if any, of these formulations would yield meaningful information about the value of adequate and reasonable data security. However, even taken at face value, these questions would raise concerns about how seriously consumers—who may not be well-versed in evaluating data security when purchasing health insurance—would consider plans whose security “falls short of industry standards,” or does not adhere to “fundamental data security practices.”²⁶ Thus, if a survey approach cannot offer a “but-for” product option that is plausible in the real world, it may not yield results that offer insight into the relevant question.

26. Greg M. Allenby, Jeff D. Brazell, John R. Howell, & Peter E. Rossi, *Economic Valuation of Product Features*, 12 QUANTITATIVE MARKETING AND ECON. 421, 433 (2014) [hereinafter Allenby et al., *Economic Valuation*] (“[T]he conjoint exercise makes the consumers (survey respondents) aware of the new product features and assumes that all choice alternatives are, hypothetically at least, available for purchase.”).

IV. “P-R-I-V-A-C-Y IS PRICELESS TO ME”²⁷: CAN CONJOINT ANALYSIS IDENTIFY AN ECONOMICALLY OBJECTIVE VALUE OF THE RELEVANT FEATURE?

Even if a conjoint survey is designed to elicit information about a complex and abstract concept like adequate and reasonable data security, a relevant next question is what value exactly that analysis would be estimating. In considering the answer to this question, it is important to keep in mind that the economic damages award should return plaintiffs to the financial positions they would have occupied in the absence of the allegedly unlawful actions. To assess what positions those would have been, it is necessary to estimate the but-for prices of the products at issue. A key feature of conjoint analysis, however, is that it estimates a consumer’s self-reported *willingness to pay* for something. The consumer’s willingness, however, is just one side of the equation that determines prices. What prices a seller is willing to accept, which conjoint analysis does not address, also plays a role in determining but-for prices.

As an initial matter, surveys used in a conjoint analysis solicit from respondents their subjective valuations of various product features. Perceptions of “value” may differ based on respondents’ individualized preferences, their varying knowledge about the features and products at issue, their budget constraints, and the specific alternatives available to each of them.²⁸ However, despite different perceptions of “value,” two customers purchasing the same product from the same seller at the same point in time would generally pay the same or similar prices. This means that a consumer’s *valuation of a product* is not the same as the *price of that product*.²⁹ Recognizing the distinction between *perceived value* and

27. PEARL JAM, VITALOGY (Epic Records 1994). *See also* Al Weisel, *Vitalogy*, ROLLING STONE (Dec. 15, 1994, 5:00 AM), <https://www.rollingstone.com/music/albumreviews/vitalogy-1994121> (“‘Pry, To’ is a one-minute doodle that consists of [Eddie] Vedder spelling out the word *privacy* over and over until we get the point already.”).

28. For example, a higher-income consumer may be willing to pay more for “data security” as part of a health insurance product than a lower-income consumer. This does not mean, however, that if the two customers purchased the same product, the higher-income customer necessarily paid a higher price. *See, e.g.*, Paul G. Patterson & Richard A. Spreng, *Modelling the Relationship Between Perceived Value, Satisfaction and Repurchase Intentions in a Business-to-Business, Services Context: An Empirical Examination*, 8 INT’L J. SERV. INDUSTRY MGMT. 414, 416 (1997).

29. As a matter of economics, for each purchaser, as well as for all purchasers collectively, the “value” of a product necessarily equals or exceeds the prevailing price, since no potential consumer who gets less “value” than the amount of the price would purchase it. The difference between consumers’ “willingness to pay” (or perceived “value”) and the prevailing price is called as “consumer surplus” and is a basic concept in economics. *See, e.g.*, N. GREGORY MANKIW, PRINCIPLES OF ECONOMICS 139 (7th ed. 2015).

prevailing price is essential in assessing a benefit of the bargain claim in a data breach class action. Consider the following illustrative example:

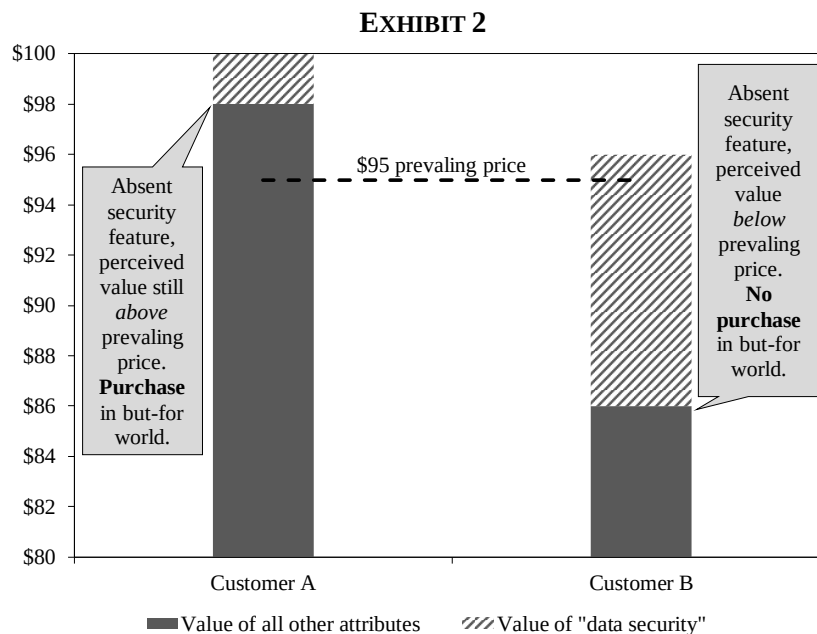
Based on the features of a particular health insurance product (e.g., monthly premium, hospital choice, adequate and reasonable data security, etc.), Customer A has a subjective “value” of \$100 for that product. If Customer A can purchase the product for \$95, the difference between value and price—i.e., the “consumer surplus”—is \$5.

Now suppose that Customer A has a subjective “value” of \$2 for the “data security” feature. If Customer A did not, in fact, get the “benefit of the bargain,” then the value he received was \$98 and not \$100. However, because even the diminished value is above the prevailing price of \$95, Customer A would still buy that product in the but-for world.

Now consider another—more security-conscious—Customer B:

Customer B has a subjective “value” of \$96 for the identical health insurance product, and a \$10 value for the “data security” feature. In the actual world, Customer B would buy the product because the value to her (\$96) is greater than the prevailing price (\$95). The consumer surplus for Customer B in the actual world is \$1. However, in the but-for world where the \$10 “data security” feature is excluded, Customer B would *not* pay \$95 for \$86 of value.

Exhibit 2 summarizes this example.



This example illustrates several key issues with conjoint analysis.

First, while the two customers have different perceptions of “value” (both for “data security” and for the product as a whole), there is only a single prevailing price: \$95. Their individual preferences only determine whether they buy the product or not, not the price they pay.

Second, while Customer A received less “value” than he would have in the but-for world, he would still have purchased the product absent the “data security” feature (i.e., price of \$95 versus \$98 in value). That is, Customer A would have still paid \$95 for this product even if the “bargain” did not include the “benefit” of data security. However, given Customer B’s preferences, that customer would *not* have purchased the product in the but-for world.

Third, even if each customer’s preferences for “data security” could be measured objectively, an average of \$6 (Customer A’s value of \$2 and Customer B’s value of \$10) would be misleading. This is because it would falsely imply that the Customer A *would not* have purchased this product in the but-for world (i.e., price of \$95 versus \$94 in value).³⁰

Ultimately, neither customer’s perceived valuation of product features solely dictates the actual price charged by the seller. Thus, as this example shows, using conjoint analysis to estimate consumers’ subjective values of product features is not the same as studying prices that would have prevailed, but for the alleged illegal conduct (i.e., whether the hypothetical insurance product would have been priced at anything other than \$95 even absent the “data security” feature).

Determining but-for prices requires an analysis of how, if at all, the product’s “market-clearing” price would have changed in the absence of the allegedly illegal conduct. However, prices are determined not solely by what consumers are willing to pay but also by what sellers are willing to accept. If properly designed and implemented, a conjoint survey may provide an estimate of consumers’ willingness to pay for a product relative to their willingness to pay for a similar product that has slightly different features. At best, this addresses the “demand” side of the equation. It cannot, however, offer insight into how, if at all, the seller of the product (or its competitors) would change its prices.

Consider again the example of the \$95 health insurance product. While it may be that consumers would reduce their willingness to pay for

30. The example can be further complicated by adding a third customer—risk-loving Customer C—who values “data security” at \$0. Applying the average perception of “value” to Customer C would falsely impute *any* decline in received value from the removal of this feature.

it if certain features were removed, that finding offers no insight into what price the seller would charge. For example, if supply-side competition is vigorous because many other sellers offer many similar products at similar prices, the removal of a valued feature may lead to a reduction in price. If competition is not as vigorous or products are sufficiently differentiated, it may be that the seller does not reduce the price it charges even if the feature is removed.³¹ Moreover, if the seller is able to set pricing at different levels for different groups of customers based on characteristics of their demand for this product, it may be that the price charged to some (but not all) customers would change as a result of removing a feature. Nonetheless, simply assuming that a reduction in consumers' "value" would necessarily correspond to an identical reduction in price ignores the supply-side factors that determine prices.

Academic literature on survey-based methods, including conjoint analysis, indicates that these methods may produce estimates of "willingness to pay" that are higher than the prices that would prevail in a real-world setting. As one paper on implementation of conjoint analysis notes³²:

In the context of conjoint studies, feature valuation is achieved by using various *measures that relate only to the demand for the products and features and not to the supply*. In particular, it is common to produce estimates of what some call Willingness To Pay and Willingness To Buy. Both WTP and WTB depend only on the parameters of the demand system. As such, *the WTP and WTB measure cannot be measures of the market value of a product feature* as they do not directly relate to what incremental profits a firm can earn on the basis of the product feature.

The same paper states that measures of willingness to pay derived from conjoint surveys³³:

[D]o not take into account equilibrium adjustments in the market as one of the products is enhanced by addition of a

31. In this instance, the survey respondent's hypothesized valuation of the relevant feature is irrelevant to the but-for world. That is, if the product is priced the same whether it has the feature at issue or not, the but-for price is the same, even if the consumer perceives receiving less "value." This outcome may occur in a market for differentiated products, often characterized by substantial investments by sellers on branding and advertising. See, e.g., B.C. Giri et al., *Multi-Manufacturer Pricing and Quality Management Strategies in the Presence of Brand Differentiation and Return Policy*, 105 *COMPUTERS & INDUS. ENGINEERING* 146 (2017).

32. Greg M. Allenby et al., *Using Conjoint Analysis to Determine the Market Value of Product Features*, in *PROCEEDINGS OF THE SAWTOOTH SOFTWARE CONFERENCE ON PERCEPTUAL MAPPING, CONJOINT ANALYSIS AND COMPUTER INTERVIEWING* 343 (2013) (emphasis added).

33. *Id.* at 346–47 (emphasis added).

feature. For this reason, we cannot view either pseudo-WTP nor WTP as what a firm can charge for a feature-enhanced product nor can we view WTB as the market share than can be gained by feature enhancement. Computation of *changes in the market equilibrium* due to feature enhancement of one product will be required to develop a measure of the economic value of the feature. *WTP will overstate the price premium afforded by feature enhancement and WTB will also overstate the impact of feature enhancement on market share.*

Absent such a “computation of changes in market equilibrium,” a conjoint analysis cannot answer the question relevant for the determination of impact and damages. That is, what prices would plaintiffs have paid for the “bargain” they received from defendants? Rather, this approach considers only one side of the price-setting equation and necessarily overstates the impact (if any) of the foregone “benefit” on prices. Conjoint analysis does not study actual transactions engaged in between plaintiffs and defendants, and by considering only part of the equation, on its own, it cannot account for an important part of the real-world price-setting process.³⁴

This feature of conjoint analysis proved relevant in a number of false claims class actions. For example, the *NJOY* court did not certify the proposed class of e-cigarette purchasers because the plaintiffs’ expert’s conjoint analysis did not satisfy *Comcast*³⁵: “His conjoint methodology could quantify the relative value a class of consumers ascribed to the safety message, but it does not permit the court to turn the relative valuation into an absolute valuation to be awarded as damages.” Similarly, the *Saavedra* court declined to certify the proposed class of consumers because the proposed conjoint analysis—which was neither designed nor executed at the time of the class certification decision—“focuse[d] only on the demand side of the equation” and “suffer[ed] from serious methodological flaws.”³⁶

34. See Greg M. Allenby et al., *Computing Damages in Product Mislabeling Cases: Plaintiff’s Mistaken Approach in Briseno v. ConAgra*, 45 PROD. SAFETY & LIAB. REP. 208 (2017) (“[I]t is important to remember that consumer valuations of the misrepresented feature are not the same as the market price premium associated with the alleged misrepresentation . . . If the analysis employed does not also account for costs and other market forces such as competition among suppliers, the resulting damages estimates may be significantly overstated.”).

35. Order Denying Plaintiffs’ Amended Motion for Class Certification at 8, *In re NJOY, Inc. Consumer Class Action Litigation*, 120 F. Supp. 3d 1050 (C.D. Cal. Aug. 14, 2015), ECF No. 325.

36. *Saavedra v. Eli Lilly & Co.*, No. 2:12-cv-9366-SVW, 2014 U.S. Dist. LEXIS 179088, at *11, *18, *33 (C.D. Cal. Dec. 18, 2014) (involving alleged misrepresentations regarding risk

To address the limitation of conjoint analysis as a “demand-side” tool, some practitioners have suggested a variation on the basic approach. Specifically, some practitioners have suggested that “if the researcher seeks qualitative information about how much consumers value . . . the attribute at issue, he can develop a conjoint survey that provides that average or median consumer WTP.”³⁷ In contrast, “if the researcher wants to assess the price premium associated with the [attribute at issue], then he will need to develop a conjoint survey that assesses the WTP of the marginal consumer—i.e., the consumer who is indifferent between buying and not buying the . . . product.”³⁸

Using the “marginal” willingness to pay to assess a “price premium” for the feature at issue is based on the notion that the marginal consumer’s willingness to pay is equal to the market-clearing price for a product. That is, if the price were any higher, it would be above that consumer’s willingness to pay. As a result, the idea is that taking the difference between the actual price of a product and the ostensibly market-clearing price for the product without the feature at issue can be used to determine the value of the feature.

This distinction between average and marginal WTP played a role in the *Dial* case, where the court certified a proposed class of soap purchasers and indicated that³⁹:

[W]hile no doubt imperfect in some respects, weak in others, and subject to challenges on cross-examination, [Plaintiffs’ expert’s] proffered means of calculating class wide damages is sufficient to demonstrate that a price premium for the allegedly falsely-claimed feature(s) exists, and that it can be reliably calculated, using means and methods generally understood and accepted in the fields of economics and statistics.

Specifically, the court noted that by determining the marginal consumer’s willingness to pay for the product without the feature at issue, plaintiffs’ expert’s model purportedly also determined the maximum price [at which

of experiencing withdrawal symptoms upon discontinuation of using Eli Lilly’s antidepressant, Cymbalta).

37. Lisa Cameron et al., *The Role of Conjoint Surveys in Reasonable Royalty Cases*, LAW360 (Oct. 16, 2013), <https://www.law360.com/articles/475390/the-role-of-conjoint-surveys-in-reasonable-royalty-cases>.

38. *Id.* (“It is the WTP of the marginal consumer that is equivalent to the price premium associated with the infringing level of the attribute; this marginal consumer can be identified by offering respondents a ‘no buy’ option.”).

39. *In re Dial Complete Mktg. & Sales Practices Litig.*, 320 F.R.D. 326, 337 (D.N.H. 2017).

Dial] could “have sold the equivalent number of products without the false claim(s).”⁴⁰

This model, however, only appears to have addressed the supply-side issue by assuming it away.⁴¹ In estimating the marginal consumer’s willingness to pay for the but-for product, plaintiffs’ expert in *Dial* “held constant” the quantity, i.e., “the number of products with the offending claims actually sold.”⁴² This assumed that Dial’s goal was to sell a fixed number of soap bars, and in the absence of the feature at issue, it would have had to lower its price in order to sell that number.⁴³ This is a strong assumption, however. As discussed above, the but-for price depends on the behavior of suppliers, and it may be that even in the absence of the feature at issue, the same “market-clearing” price would prevail. A “fixed quantity” cannot simply be assumed; rather, any assumptions about but-for quantities should be supported through sound economic analysis.

Notably, the assumption that if a feature were removed from a product, sellers would simply reduce the price of that product by the value of that feature (or by any amount) may be inconsistent with how price-setting works in the real world. For example, as an alternative to the but-for world offered by the *Dial* plaintiffs’ expert, a seller could choose to keep prices unchanged, allowing for fewer consumers to purchase the allegedly lower-quality product.⁴⁴ Depending on the industry at issue, sellers may also use a variety of pricing strategies that do not rely on valuation of features at all. For example, some retailers may use “line pricing,” a strategy that assigns a uniform list price to a group of similar products, even if the exact features of those products vary.⁴⁵ In other instances, retailers may use “focal point pricing,” whereby products are

40. *Id.* at 336–37.

41. Notably, whether a conjoint analysis relies on the average, median, or marginal consumer does not address the issue described above. That is, it appears to be ill-suited for valuation of abstract product features such as “data security.”

42. *In re Dial*, 320 F.R.D. at 336.

43. Put differently, Dial chooses a price that will yield sales of X soap bars. In the presence of the false label, Dial can sell X soap bars at the price of \$Y. However, once the false label is removed, Dial can no longer sell X soap bars—because some customers are no longer willing to pay \$Y—and must therefore reduce the price to sell the target number of units. This price reduction would represent harm from the false claim.

44. In this scenario, damages for some consumers (i.e., those who would continue to purchase the allegedly lower-quality product at the same price) would be zero. Consumers who would choose *not* to buy the product in this but-for world would be injured, but the amount of damages would depend on a given consumer’s second-best available option.

45. See, e.g., *Weiner v. Snapple Beverage Corp.*, No. 07 Civ. 8742(DLC) 2010 U.S. Dist. LEXIS 79647, at *3 (S.D.N.Y. Aug. 3, 2010).

priced at dollar levels ending in “9” or cent levels ending at “99.”⁴⁶ Under these kinds of pricing strategies, among others, the prices consumers pay may not change even if the features of a product do—a reality inconsistent with the foundational assumption of conjoint analysis.⁴⁷

Plaintiffs’ expert in *Anthem* also recognized this shortcoming of the willingness-to-pay analysis, emphasizing that “market price is determined not only by consumer demand and willingness to pay for a product feature but also by competition from other manufacturers” and that “a market price premium therefore differs from willingness to pay because it is what a firm can charge for a product with a particular feature rather than just the consumers’ valuation of that product feature.”⁴⁸ However, he did not actually conduct an empirical analysis to address this issue. Rather, he indicated that “with some analysis on the supply side, it is possible to compute Nash equilibrium prices for health insurance products associated with a range of data security levels.”⁴⁹ Additionally, *Anthem* plaintiffs’ expert cited to an academic article he had written,⁵⁰ which he suggested provided “sufficient detail” on the “mathematical details of [his] proposed methodology.”⁵¹ Nonetheless, no market price premia were actually derived in *Anthem*, as neither a conjoint analysis nor a Nash equilibrium analysis were conducted. Thus,

46. See, e.g., Eric T. Anderson & Duncan I. Simester, *Effects of \$9 Price Endings on Retail Sales: Evidence from Field Experiments*, 1 *QUANTITATIVE MARKETING AND ECON.* 93 (2003); Robert M. Schindler & Patrick N. Kirby, *Patterns of Rightmost Digits Used in Advertised Prices: Implications for Nine-Ending Effects*, 24 *J. CONSUMER RES.* 192 (1997); Mark Stiving & Russell S. Winer, *An Empirical Analysis of Price Endings with Scanner Data*, 24 *J. CONSUMER RES.* 57 (1997).

47. See, e.g., Allenby et al., *Economic Valuation*, *supra* note 26, at 429 n.6 (“In a conjoint setting, we abstract from the problem of omitted characteristics as the products we use in our market simulators are defined only in terms of known and observable characteristics. Thus, the standard interpretation of the market wide shock is not applicable here. Another interpretation is that the market wide shock represents some sort of marketing action by the firms (e.g. advertising). Here, we are directly solving the firm pricing problem holding fixed any other marketing actions.”).

48. Rossi Report, *supra* note 25, at 27–28.

49. Rossi Report, *supra* note 25, at 46.

50. Reply Expert Report of Peter E. Rossi at 9 n.9, *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK (N.D. Cal. May 5, 2017) (citing Allenby et al., *Economic Valuation*, *supra* note 26). Notably, this article outlines a series of assumptions upon which its theory is based. Determining whether these assumptions hold for a particular product or industry at issue in a litigation would require an inquiry into the facts of the specific case. Additionally, as the authors point out, “there is no guarantee that a Nash equilibrium exists for heterogeneous logit demand.” Allenby et al., *Economic Valuation*, *supra* note 26; see also Greg M. Allenby et al., *Valuation of Patented Product Features*, 57 *J. L. & ECON.* 629 (2014).

51. Reply Expert Report of Peter E. Rossi at 9, *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK (N.D. Cal. May 5, 2017).

whether this type of analysis can yield meaningful results in a real-world data breach litigation remains an open question.⁵²

V. “ALL FOR ONE AND ONE FOR ALL”: CAN CONJOINT ANALYSIS BE USED TO SHOW A BREACH’S IMPACT ON ALL (OR NEARLY ALL) PROPOSED CLASS MEMBERS?

Cohen et al., discussed several key elements of constructing an appropriate “but-for world” in data breach class actions, including testing (and “falsifiability”) of assumptions, as well as rigorous assessment to determine whether injury can be established using evidence common to the proposed class.⁵³ Moreover, there are potential problems with using a sample intended to represent the “average” or “typical” experience of the proposed class, specifically⁵⁴: “[g]iven consumers’ idiosyncratic reactions to a data breach, extrapolating from a small sample of consumers to thousands (or millions) of other purported class members whose data was (or may have been) compromised risks reaching the wrong conclusions.”⁵⁵

Relying on conjoint analysis in the context of assessing a benefit of the bargain claim may face this exact issue. In the context of the “willingness-to-pay” approach, the issue of conjoint analysis as “common proof” relates to the factual question of whether some class members place a high value on this feature, while others give it little or no value. This is not simply an issue of imprecisely estimating damages for a given class member (i.e., one class member valuing adequate and reasonable data security at \$2 and another at \$10, and therefore the average of \$6 not precisely compensating either one). Rather, this approach runs the risk of improperly estimating damages for unharmed customers or, potentially, failing to find damages for class members who were harmed. In fact, although conjoint analysis would yield a single aggregate valuation for adequate and reasonable data security, responses

52. Allenby et al., *Economic Valuation*, *supra* note 26, at 440 (“[T]he quality standards for design and analysis of conjoint data have to be much higher when used for economic valuation than for many of the typical uses for conjoint.”).

53. Cohen et al., *supra* note 6, at 3.

54. Notably, to yield meaningful information from which survey results can be extrapolated to the population at issue, the survey should be properly designed, and the population properly sampled. *See, e.g.*, Allenby et al., *Valuation of Patented Product*, *supra* note 52, at 641 (“Considerations of sample representativeness are critical to the reliability and generalizability of any survey, conjoint or otherwise. No survey evidence should be considered admissible or relevant unless evidence of representativeness is provided.”).

55. Cohen et al., *supra* note 6, at 4.

for sub-groups of respondents may indicate substantial variation,⁵⁶ including some respondents' choices indicating that they do not value this feature at all.⁵⁷ Importantly, groups (or individuals) who indicate that they do not value data security would not be harmed under a benefit of the bargain theory. That is, the "bargain" those consumers got would have allegedly lacked a "benefit" they did not value, meaning that their willingness to pay for a product which explicitly excluded that feature would have been unchanged.

This issue may be partially, though not entirely, mitigated by a "market price premium" approach like that proposed by *Anthem* plaintiffs' expert. That is, if it can be determined that the alleged conduct inflated the prevailing price of a product by some amount, it would not matter to the determination of impact and damages whether that amount is equal to a given consumer's valuation of the feature at issue. Consider again the hypothetical situation illustrated in Exhibit 2. If it can be shown, for example, that the market price premium for data security was \$1—and the prevailing but-for price would therefore have been \$94—that amount would apply to all consumers that would have bought that product in the but-for world, including Customer A (despite that customer *personally* valuing data security at \$2).⁵⁸

The issue that persists even with the market price premium approach is that in the real world, there may not be a single product or a single price premium that is relevant to the assessment of harm for the entire proposed class. For example, while the plaintiffs' expert in *Anthem* provided an extended discussion of how healthcare pricing varies substantially across geographies, product offerings, and customer segments—and, indeed, of how "prices" consumers pay can be a complex combination of premiums, deductibles, copayments, and coinsurance⁵⁹—he nonetheless concluded that a "market price" can be used to show that "all class members have suffered the same loss commensurate or proportional to the price paid by

56. For example, attitudes toward, and preferences for, data security may vary across consumers depending on age, educational attainment, income, or other factors. *Id.* at 6.

57. *See id.* In fact, an improperly designed conjoint analysis may indicate that respondents are "irrational" and place a *negative* value on data security. Improperly designed conjoint analyses may also indicate an unreasonable range in the valuation of the feature at issue, including some respondents valuing the feature above the total price of the product. However, if the aggregation of all results—even unreasonable ones—yields a positive valuation, the conclusion would be that the positive valuation was "common" to the class.

58. Notably, the security-conscious Customer B would not have purchased the but-for product for \$94, meaning the improperly defined "bargain" induced that consumer to purchase a product she otherwise would not have.

59. Rossi Report, *supra* note 25, at Section III.

them.”⁶⁰ Moreover, he indicated that he would “undertake surveys of different markets” and that these surveys would be “analyzed independently to determine market price premia in each of these distinct markets.”⁶¹

However, even this approach—to the extent proof in the form of many distinct market-specific analyses may be considered “common” to the proposed class—would assume that there was a single data security premium within a given “market.” That is, even a “market-specific” survey, by construction, would imply only two possible outcomes: either every consumer in that market was injured—and necessarily in the same amount—or no consumer was injured. However, to the extent price premia for data security vary across geographies, product offerings, and customer segments within markets (as defined by the survey designer), such surveys would (potentially inappropriately) assume that price premiums are identical across these parameters. Requisite testing of such an assumption would be necessary to determine whether it is appropriate given the facts of the case at hand.

60. *Id.* at 26.

61. *Id.* at 23.

CHILD PRIVACY IN THE DIGITAL AGE AND CALIFORNIA'S CHILD DELETION STATUTE

*Michael Shepherd**

INTRODUCTION	134
I. BRIEF HISTORY OF CHILD PRIVACY.....	135
II. RECENT CASE LAW CONCERNING CHILD PRIVACY ON SOCIAL MEDIA	137
III. CRITIQUE OF RECENT CASE LAW	139
IV. CALIFORNIA'S CHILD DELETION STATUTE	140
V. COMMERCE CLAUSE CHALLENGES TO THE STATUTE	141
VI. SOLUTIONS TO THE COMMERCE CLAUSE CHALLENGES	143
VII. STATUTE IN CONFLICT WITH FREE SPEECH.....	143
VIII. STATUTE'S LIMITS ON HELPING REVENGE PORN VICTIMS	144
IX. STATUTE'S LIMITS FOR ASPIRING COLLEGE STUDENTS AND EMPLOYEES	144
CONCLUSION.....	145

INTRODUCTION

In the current era of social media, parents and others constantly post pictures and reveal information about children on the Internet. As of 2010, ninety-two percent of children had an online presence by the age of two.¹ This Note will examine whether parents and others' use of social media infringe on the privacy rights of children and what protections a recent California statute gives to children's digital privacy.

A recent case sheds light on this emerging issue. In *Sakala v. Milunga*, the plaintiff alleged the defendants induced her to come to the United

* B.S., United States Military Academy at West Point (2011); J.D. Candidate, University of Florida Levin College of Law (2019). I am grateful to all the individuals who helped with this Note to include my classmates on the Journal of Technology Law & Policy Executive Board and Professor Stacey Steinberg, who initiated my interest in this topic.

1. See *Digital Birth: Welcome to the Online World*, BUS. WIRE (Oct. 6, 2010, 1:02 PM), <http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth-Online-World>.

States from Zambia and then held her as an involuntary servant for nearly ten months.² In November 2014, the plaintiff accepted an offer to work for the defendants for one year, which included caring for their minor son.³ During this time, the plaintiff took prosaic photographs of the child and posted them on Facebook.⁴ The plaintiff was never paid for any work she performed for the defendants.⁵ Thus, the plaintiff sought damages in federal court from the defendants under international, federal, and Maryland state law.⁶

The defendants counterclaimed.⁷ Among the six counts raised in the counterclaim, the last count alleged that the plaintiff infringed on the defendants' right of privacy by publishing pictures of their minor child on Facebook without consent.⁸ The district court dismissed all six counterclaims, stating that each "fail to allege essential elements, are stated in conclusory fashion, and rely on rampant speculation."⁹ The dismissal of the privacy claim was based on historic child privacy laws that were not tailored to the digital age.¹⁰

I. BRIEF HISTORY OF CHILD PRIVACY

Privacy rights of children historically concerned only child celebrities. In *Sidis v. F-R Publishing Corp.*, the plaintiff was a national celebrity as a child in the early 1900s.¹¹ In 1937, *The New Yorker* published an article that included sketches of Sidis as a child.¹² Sidis sued the magazine, arguing that he had a right to privacy under state law.¹³ The court disagreed, holding that Sidis's life was a "matter of public concern" because of his fame as a child.¹⁴

Almost forty years after *Sidis*, the Restatement (Second) of Torts included the invasion of the right to privacy.¹⁵ An invasion of the right to privacy could be found in four circumstances: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of the other's name or

2. Complaint at 1, *Sakala v. Milunga*, No. 8:16-CV-00790-PWG, (D. Md. Mar. 17, 2016).

3. *Id.* at 2.

4. *Sakala v. Milunga*, No. PWG-16-790, 2017 WL 2986364, at *4 (D. Md. July 13, 2017).

5. Complaint, *supra* note 2, at 4.

6. *Id.* at 1.

7. Defendant's Answer to Plaintiff's Second Amended Complaint at 26, *Sakala v. Milunga*, No. 8:16-CV-00790-PWG (D. Md. Dec. 8, 2016).

8. *Id.* at 44–45.

9. *Sakala*, 2017 WL 2986364, at *4.

10. *See id.*

11. *Sidis v. F-R Pub. Corp.*, 113 F.2d 806, 807 (2d Cir. 1940).

12. *Id.*

13. *Id.* at 808.

14. *Id.* at 809.

15. RESTATEMENT (SECOND) OF TORTS § 652A (AM. L. INST. 1977).

likeness; (3) unreasonable publicity given to the other's private life; (4) or publicity that unreasonably places the other in a false light before the public.¹⁶ These four forms of invasion are cemented in American courts and are actionable under tort liability.¹⁷

Because this tort was recognized before the Internet, it mainly focuses on providing a remedy to someone whose privacy was invaded by the press. Additionally, there are no existing cases where a child has sued a parent or other adult under this tort.¹⁸ This is most likely due to the child-parent immunity doctrine.¹⁹ Nonetheless, the invasion of a child's privacy now had an avenue for seeking a remedy.

However, a child's remedy for invasion of privacy may be severely limited by their fame or lack thereof.²⁰ In *Lawrence v. A.S. Abell Co.*, a woman consented to a photographer from a local newspaper taking a photograph of her infant and her friend's infant while at a festival.²¹ The next day, photographs of the infants appeared on the front page of the newspaper with a caption indicating their names, ages, and the location where the photographs were taken.²² About six weeks later, the newspaper began an advertising campaign that included the infants' photographs on billboards, commercials, and rack cards.²³ The mothers of the infants sought compensation based on invasion of privacy and unjust enrichment.²⁴ The Court of Appeals of Maryland applied the Restatement (Second) of Torts' four forms of invasion of privacy.²⁵ The court held that the republishing of the children's photographs was not actionable because the infants' name or likeness did not have "commercial or other value."²⁶ Thus, a newspaper republishing photographs of infants who were ordinary members of the public and were taken in a public place was insufficient to rise to the level of the tortious act of invasion of privacy.²⁷

Moreover, a child's consent is especially irrelevant when that child is a public figure.²⁸ In *Heath v. Playboy Enterprises*, a woman brought a

16. *Id.*

17. *Id.*

18. Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 841, 874 n.255 (2017).

19. *Id.*

20. *Lawrence v. A.S. Abell Co.*, 475 A.2d 448, 453 (Md. 1984).

21. *Id.* at 449.

22. *Id.*

23. *Id.*

24. *Id.*

25. *Id.* at 451.

26. *Id.* at 453.

27. *Id.*

28. *Heath v. Playboy Enters., Inc.*, 732 F. Supp. 1145, 1150 (S.D. Fla. 1990).

paternity action against a celebrity talk show host's adult son.²⁹ Playboy published a photograph of the woman and her minor child outside of a county courthouse following a hearing.³⁰ The child's guardian ad litem then filed a complaint of invasion of privacy.³¹ The plaintiff argued that Playboy should not have published the photograph without the child's consent.³² The *Heath* court explained that consent is only relevant when there is an issue regarding the plaintiff's status as a public figure, the legitimacy of public concern, or the disclosure of private facts.³³ Thus, the court held the child did not have an actionable claim because she was a public figure who had a national following and the photograph was taken in a public place after an event open to the public.³⁴

These cases demonstrate the challenges of pleading an actionable claim for the invasion of a child's privacy before the Internet. With the creation of social media sites such as Facebook in 2004,³⁵ photographs and personal information of children can now be shared throughout the digital world. Further, children have no control over what their parents post or share about them on social media.³⁶ The following cases demonstrate how courts have applied the invasion of privacy to children on social media.

II. RECENT CASE LAW CONCERNING CHILD PRIVACY ON SOCIAL MEDIA

A user's privacy settings on social media, regardless of their age, can severely limit the user's right of privacy.³⁷ In *Chaney v. Fayette County Public School District*, a county school district gave a PowerPoint presentation called "Internet safety."³⁸ One of the slides contained a photograph, obtained from Facebook, of the seventeen-year-old plaintiff.³⁹ The county school district was able to find the photograph because the plaintiff had chosen a semi-private Facebook setting that allowed her Facebook "friends" and "friends of friends" to view her page and pictures.⁴⁰ As a minor, this was the most inclusive privacy setting

29. *Id.* at 1146.

30. *Id.*

31. *Id.* at 1147.

32. *Id.* at 1149.

33. *Id.* at 1150.

34. *Id.*

35. Nicholas Carlson, *At Last—The Full Story of How Facebook Was Founded*, BUS. INSIDER (Mar. 5, 2010, 4:10 AM), <http://www.businessinsider.com/how-facebook-was-founded-2010-3>.

36. See Steinberg, *supra* note 18, at 844.

37. *Chaney v. Fayette Cty. Pub. Sch. Dist.*, 977 F. Supp. 2d 1308, 1316 (N.D. Ga. 2013).

38. *Id.* at 1312.

39. *Id.*

40. *Id.* at 1313.

available.⁴¹ Neither the plaintiff nor her parents consented to the county's use of the photograph.⁴² The court explained that "[b]y intentionally selecting the broadest privacy setting available to her at that time, Chaney made her page available to potentially hundreds, if not thousands, of people she did not know (i.e., the friends of her Facebook friends)."⁴³ Thus, the plaintiff forfeited any reasonable expectation of privacy concerning her Facebook profile.⁴⁴

Further, the court held the plaintiff's status as a minor did not magnify her right of privacy.⁴⁵ *Chaney* demonstrated that a child can implicitly surrender his or her reasonable expectation of privacy through the privacy settings the child chooses on his or her social media account. However, the case does not address the privacy rights of children when their information and images are posted on the Internet without their expressed or implied consent.

Parents are in complete control of their minor child's privacy on social media.⁴⁶ In *Thomas v. Cash*, a minor child's adoptive parents sought a protective order from the child's biological family because they posted pictures of the minor child on their Facebook accounts.⁴⁷ The trial court entered a protective order for five years against each defendant on grounds of harassment, ordering that the defendants were "not to post or display any photograph of the minor child or the child's parents . . . or make any comments about any of them on any social media or to the petitioners or to any public site."⁴⁸ The trial judge explained that he saw "no valid purpose" to post photographs of the child; the only purpose was harassment.⁴⁹ The appellate court reversed and lifted the protective order, explaining that the parents caused the invasion of their child's privacy.⁵⁰ Because the legal parents posted photographs of the minor child on their Facebook accounts and allowed others to do the same, the biological family could permissibly download those photographs and post them on their Facebook accounts.⁵¹

In *Sakala*, as in *Thomas*, the court had to consider the privacy rights of a child who did not consent to photographs of himself being posted on

41. *Id.*

42. *Id.*

43. *Id.* at 1315.

44. *Id.* at 1316.

45. *Id.*

46. See *Thomas v. Cash*, 423 P.3d 670, 676 (Okla. Civ. App. 2016).

47. *Id.* at 672.

48. *Id.* at 674.

49. *Id.*

50. See *id.* at 676.

51. See *id.* at 677.

social media.⁵² The court determined that the claimed invasion of privacy did not fall into one of the four forms of the invasion of privacy tort from *Lawrence* and the Restatement (Second) of Torts.⁵³ The photographs that Sakala posted of the minor child on Facebook were ordinary.⁵⁴ They included trips to the White House and the beach, a ride on the subway, and candid ones in a home.⁵⁵ Thus, the photographs were not sufficient for a privacy invasion counterclaim because they did not disclose anything about the minor child that was not readily observable by the public whenever the child went out into the world with his parents.⁵⁶

III. CRITIQUE OF RECENT CASE LAW

Sakala and *Thomas* were decided under the traditional reasoning given in *Lawrence* and *Heath* that factored a child's fame into his or her right of privacy. New statutes will need to be created to appropriately address a minor child's privacy in the digital age. *Sidis* demonstrated the difficulties of adults to reclaim their privacy rights that were forfeited by others when they were children. Historically, this has only been an issue for minor celebrities. Times have changed. When current minors become adults, an increasing ninety-two percent of them will already have had their personal information and photographs disseminated to unknown places and people.⁵⁷

Both the *Sakala* and *Thomas* courts did not consider what the minor child might want regarding his or her digital footprint. Even though the postings of photographs of the child did not constitute harassment in *Thomas*,⁵⁸ those actions should still be considered invasions of the child's privacy because the child never consented to those photographs being posted on Facebook. Similarly, while the photographs in *Sakala* may have been ordinary and their depictions readily observed by the public, the decision to post the photographs should ultimately reside with the person who is in the photograph. This will alleviate issues that parents' oversharing are causing, such as digital kidnapping, online bullying, and even the possibility that one day, adults will want to change their names because of the embarrassing content shared online from their minor years.⁵⁹

52. See *Sakala v. Milunga*, No. PWG-16-790, 2017 WL 2986364, at *4 (D. Md. July 13, 2017).

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

57. See *Digital Birth: Welcome to the Online World*, *supra* note 1.

58. *Thomas v. Cash*, No. 113642, 2016 WL 8377118, at *7, (Okla. Civ. App. Aug. 25, 2016).

59. See Steinberg, *supra* note 18, at 854–55.

Therefore, privacy rights of children in the current age of social media need protection through new statutes and the courts. Historically, the privacy rights of children were only an issue when dealing with child celebrities. Though the Restatement (Second) of Torts provided a remedy, minors' privacy rights could still be forfeited by their parents. With the creation of the Internet and social media, children's privacy rights are being infringed in significantly larger numbers. Current case law, as in *Sakala*, applies an outdated framework ill-adapted to the realities of the digital age. Statutes that address parents' and other adults' infringement on minor children's privacy rights on the Internet could be passed to alleviate safety and legal risks.

IV. CALIFORNIA'S CHILD DELETION STATUTE

California has attempted to protect children's privacy rights in the digital age, but it is limited in scope.⁶⁰ A recent California bill (the Statute) allows minor children to delete their posts and establishes a minor's right to deletion.⁶¹ The Statute provides a remedy to minors like Chaney who may want to remove photographs and other information they themselves posted on social media. However, it does not give minors a deletion option with respect to what their parents or others post about them.⁶²

The main crux of the Statute permits a minor who is a registered user of an Internet Web site, online service, online application, or mobile application (Site or Sites, collectively) "to remove or, if the operator prefers, to request and obtain removal of, content or information posted on the operator's [Site] . . . by the user."⁶³ The Statute also requires a Site to provide notice to registered minors of their right to deletion⁶⁴ as well as clear instructions on how to remove content.⁶⁵ The first section of the Statute, however, limits liability to Sites that have actual knowledge that a minor is using its Site.⁶⁶

The Statute is also limited because it does not require a Site to delete content that was stored or posted by a third party.⁶⁷ Critics have commented that this limitation makes the bill inefficient because the main

60. See CAL. BUS. & PROF. CODE § 22581 (West 2015).

61. See *id.*

62. See Steinberg, *supra* note 18, at 844 n.20.

63. CAL. BUS. & PROF. CODE § 22581(a)(1).

64. *Id.* § 22581(a)(2).

65. *Id.* § 22581(a)(3).

66. *Id.* § 22581(a).

67. *Id.* § 22581(b)(2).

issue of digital child privacy concerns third parties.⁶⁸ Thus, a Site remains in compliance of the Statute even if the content “remains visible because a third party has copied the posting or reposted the content or information remains on the operator’s servers in some form.”⁶⁹ These limitations demonstrate that the purpose of the Statute was only to protect minors, who post inappropriate content as a result of their youthful immaturity, from themselves.⁷⁰

V. COMMERCE CLAUSE CHALLENGES TO THE STATUTE

While the Statute grants minors the right to deletion of content they post on Sites, the Statute may face certain constitutional constraints. James Lee argues that the Statute is unconstitutional under the dormant Commerce Clause.⁷¹ A statute discriminates against interstate commerce when it provides for differential treatment of in-state and out-of-state economic interests.⁷² Because the Statute is not limited to Sites in California, Sites in other states that service California users are forced to follow the Statute, thus violating the Commerce Clause.⁷³

In *Pike v. Bruce Church, Inc.*, the Supreme Court used a balancing test that requires state regulation affecting interstate commerce to serve a legitimate local public interest sufficient enough to warrant the burden imposed on interstate commerce.⁷⁴ Thus, the Statute must not impose a burden on interstate commerce that is clearly excessive in relation to the putative local benefits derived from the Statute.⁷⁵ Lee argues that the Statute will likely serve a legitimate local public interest⁷⁶ because California courts recognize that the state has a compelling interest in protecting minors from harm.⁷⁷ However, the Statute may still fail the *Pike* balancing test because the burden on interstate commerce outweighs the local benefits.⁷⁸

68. Eric Goldman, *California’s New ‘Online Eraser’ Law Should Be Erased*, FORBES (Sept. 24, 2013, 1:35 PM), <http://www.forbes.com/sites/ericgoldman/2013/09/24/californias-new-online-eraser-law-should-be-erased>.

69. CAL. BUS. & PROF. CODE § 22581(d)(1).

70. See Katy Steinmetz, *Lucky Kids: California Gives Minors the Right to Delete Things They Put Online*, TIME (Sept. 23, 2013), <http://techland.time.com/2013/09/23/lucky-kids-california-gives-minors-the-right-to-delete-things-they-put-online/>.

71. James Lee, *SB 568: Does California’s Online Eraser Button Protect the Privacy of Minors?*, 48 U.C. DAVIS L. REV. 1173, 1177 (2015).

72. *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 141–42 (1970).

73. See Lee, *supra* note 71, at 1177.

74. *Pike*, 397 U.S. at 142.

75. *Id.*

76. Lee, *supra* note 71, at 1191–92.

77. *Id.* at 1192.

78. *Id.* at 1193.

Because the Statute implicitly requires Sites hosted on servers outside of California to comply with the Statute,⁷⁹ Sites would either have to provide only minors in California with the ability to delete content or to provide that option to minors in all states.⁸⁰ Both options are unduly burdensome because of the huge costs to Site owners.⁸¹ Thus, a significant burden would be placed on interstate commerce.

To satisfy the first option, the Statute's supporters may cite to *National Federation of the Blind v. Target Corp.*, where the court explained that technology allows Sites to geographically locate and thus distinguish among Site users.⁸² However, while determining the nation of a Site user is very accurate, determining the city or state is much more difficult.⁸³ The court in *Target* also factored into their reasoning the fact that Sites could use a user's credit card information to determine the user's state.⁸⁴ This line of reasoning does not pertain to the Statute because Sites where minors post personal content usually do not ask for a credit card number.⁸⁵

Because of these difficulties, a Site may decide to provide California's deletion button to all users. This strategy would subject interstate commerce to inconsistent state regulation.⁸⁶ The Supreme Court held in *Pike* that this notion unduly burdens interstate commerce.⁸⁷ Therefore, the Statute does not seem to pass the *Pike* balancing test.⁸⁸

This argument is also strengthened when examining the alleged local benefit of the Statute. Deletion options already exist for primary Sites such as Facebook and Twitter.⁸⁹ Further, a minor would not benefit from the Statute if future employers and colleges could still view the minor's personal content because the content was reposted by a third party.⁹⁰

79. See CAL. BUS. & PROF. CODE § 22581 (West 2015).

80. See Goldman, *supra* note 68.

81. *Id.*

82. Nat'l Fed'n of the Blind v. Target Corp., 452 F. Supp. 2d 946, 961 (N.D. Cal. 2006).

83. See YUVAL SHAVITT & NOA ZILBERMAN, A STUDY OF GEOLOCATION DATABASES (2010), <http://arxiv.org/pdf/1005.5674v3.pdf>; *The Inside Secrets About IP Addresses and Geolocation*, WHATISMYIPADDRESS.COM, <http://whatismyipaddress.com/geolocation-accuracy> (last visited Sept. 4, 2018).

84. *Target*, 452 F. Supp. 2d at 961–62.

85. See Lee, *supra* note 71, at 1195–96.

86. *Id.* at 1197.

87. Healy v. Beer Inst., Inc., 491 U.S. 324, 337 (1989).

88. See Lee, *supra* note 71, at 1197.

89. See *How to Delete a Tweet*, TWITTER, <https://support.twitter.com/articles/18906-deleting-a-tweet> (last visited Sept. 4, 2018); *How Do I Delete a Photo I've Uploaded?*, FACEBOOK, <https://www.facebook.com/help/www/208547132518386> (last visited Sept. 4, 2018); *How Do I Hide or Delete Posts I've Shared from My Page?*, FACEBOOK, <https://www.facebook.com/help/252986458110193> (last visited Sept. 4, 2018).

90. See Lee, *supra* note 71, at 1200.

VI. SOLUTIONS TO THE COMMERCE CLAUSE CHALLENGES

One way for California to avoid a constitutional challenge is to encourage Congress to pass a national law that implements similar deletion provisions.⁹¹ This would prevent inconsistent state regulation.⁹² Sites would then have to distinguish between users in and outside of the United States,⁹³ which, as discussed previously, is fairly easy to do.⁹⁴

The United States could also pass legislation similar to the European Union's "right to be forgotten." In the EU, minors and adults may request the deletion of content relating to the user posted both personally and by third-parties.⁹⁵ Commentators explained that if this concept was limited to minors, then it might be upheld in U.S. courts.⁹⁶

A third approach is to instead focus on educating minors about the digital footprint they create when they upload personal content onto Sites.⁹⁷ Instead of a reactionary solution, educating minors would take a preventative approach. California could model their educational program on that of Common Sense Media and how it collaborates with Disney Media to educate minors about safe Internet practices on its Site and the Disney Television Channel.⁹⁸

VII. STATUTE IN CONFLICT WITH FREE SPEECH

Many commentators are curious whether the European Union's "right to be forgotten" can be implemented in the United States.⁹⁹ California's Statute seems to be moving toward the European model, but it could be encroaching on free speech.¹⁰⁰ Because there is no right to privacy in the text of the Constitution, privacy rights are not considered as fundamental as free speech rights.¹⁰¹ Thus, when the rights of privacy and free speech collide, free speech usually wins.¹⁰²

91. *Id.* at 1203.

92. *Nat'l Fed'n of the Blind v. Target Corp.*, 452 F. Supp. 2d 946, 961 (N.D. Cal. 2006).

93. *Id.*

94. *Id.*

95. See Steven C. Bennett, *The "Right to be Forgotten": Reconciling EU and U.S. Perspectives*, 30 *BERKELEY J. INT'L L.* 161, 161–63 (2012).

96. See *id.* at 166–67.

97. Lee, *supra* note 71, at 1204.

98. See *Get Cybersmart with Phineas and Ferb*, COMMON SENSE MEDIA, <https://www.commonsensemedia.org/videos/get-cybersmart-with-phineas-and-ferb> (last visited Sept. 5, 2018).

99. See Michael J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 *U. ILL. L. REV.* 1, 38 (2017).

100. *Id.* at 44.

101. See *id.* at 40; Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 *CONN. J. INT'L L.* 257, 269 (2014).

102. Kelly & Satola, *supra* note 99, at 40.

A potential reason for this difference between the European Union and the United States is that cyber privacy rights are afforded different weight in the United States and the European Union.¹⁰³ Unlike the European Union, the United States is a common law country that has over 200 years of free speech jurisprudence.¹⁰⁴ This system entrenches certain American values and concepts, which makes the process of shifting the priority of rights arduous.¹⁰⁵ Meanwhile, the European Union is dominated by civil law Member states, which makes it easier to place a higher emphasis on privacy rights.¹⁰⁶

VIII. STATUTE'S LIMITS ON HELPING REVENGE PORN VICTIMS

Regardless of the potential constitutional hurdles, the Statute is limited in various ways in protecting minors on the Internet. For example, the Statute will unfortunately be unable to assist in the revenge porn arena because of its inability to reach third parties who post content of a user. Luke Fiedler examined the laws that criminalized revenge porn.¹⁰⁷

He defined revenge porn as the “act of widely disseminating, via the Internet, nude or otherwise explicit photos or videos that were produced and exchanged while two individuals shared an intimate encounter or relationship.”¹⁰⁸ Instead of legislation, Fiedler suggests that revenge porn can be combated by Sites like Google using algorithms to detract users from going onto revenge porn Sites.¹⁰⁹ However, victims of revenge porn are faced with a web of laws, like the Statute, that unintentionally slow efforts for relief.¹¹⁰

IX. STATUTE'S LIMITS FOR ASPIRING COLLEGE STUDENTS AND EMPLOYEES

A recent study showed that of hiring managers who research the social media accounts of candidates, over one-third found content that caused them not to hire the candidate.¹¹¹ Additionally, a survey of college

103. David Meyer, *Why the EU's "Right to Be De-Linked" Should Not Go Global*, GIGAOM (Nov. 26, 2014, 7:08 AM), <https://gigaom.com/2014/11/26/why-the-eus-right-to-be-de-linked-should-not-go-global/>.

104. *Id.*

105. *Id.*

106. *Id.*

107. Luke Fiedler, *Public Shaming in the Digital Age: Are Criminal Laws the Most Effective Means to Regulate Revenge Porn?*, 34 LOY. L.A. ENT. L. REV. 155, 155 (2014).

108. *Id.*

109. *Id.* at 185–86.

110. *See id.* at 191.

111. *Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey*, CAREER BUILDER (Apr. 18, 2012),

admissions officers revealed that schools are finding more and more personal content on Facebook and Google that hurts applicants' acceptance probabilities.¹¹² The Statute seems to alleviate this problem by allowing minors to delete content they no longer wish to have on the Internet. However, the Statute does not cover adults who wish to delete content they posted as minors.¹¹³ When Californian eighteen-year-olds are applying to colleges and jobs, they will be out of luck if they did not delete content they uploaded on a site as minors before their eighteenth birthday. Thus, as stated earlier, it seems imperative to teach minors about the potential harmful effects of a digital footprint before it is too late.

CONCLUSION

Child privacy is in the new era of the Internet. Historically, child privacy only became an issue when it concerned a child celebrity. That is no longer the case. Recent case law shows that courts are attempting to fit the digital issues of modern times into an antiquated system. California's Statute seems to be a step in the right direction in helping minors remain in control of their digital footprints. However, the Statute may face some challenges and is severely limited. If the Statute unduly burdens interstate commerce by the costs it imposes on out-of-state businesses, then it could be deemed unconstitutional. Further, commentators have mentioned that the Statute is approaching an infringement on free speech by discouraging the re-posting of personal content by third parties. However, the Statute is limited because it does not protect users against third party posts, which affects revenge porn victims. The Statute does not apply to adults, including eighteen-year-olds, that are in the midst of applying to colleges and their first jobs. While the Statute is limited in many aspects, it does provide a small step in the right direction of developing new child privacy laws in the digital age.

<http://press.careerbuilder.com/2012-04-18-Thirty-Seven-Percent-of-Companies-Use-Social-Networks-to-Research-Potential-Job-Candidates-According-to-New-CareerBuilder-Survey>.

112. Russell Schaffer & Carina Wong, *Kaplan Test Prep Survey Finds That College Admissions Officers' Discovery of Online Material Damaging to Applicants Nearly Triples in a Year*, KAPLAN TEST PREP (Oct. 4, 2012), <http://press.kaptest.com/press-releases/kaplan-test-prep-survey-finds-that-college-admissions-officers-discovery-of-online-material-damaging-to-applicants-nearly-triples-in-a-year>.

113. Kurtis Alexander & Vivian Ho, *New Law Lets Teens Delete Digital Skeletons*, S.F. GATE (Sept. 24, 2013, 9:47 AM), <http://www.sfgate.com/news/article/New-law-lets-teens-delete-digital-skeletons-4837309.php>.