SOCIAL NETWORK NORMS AND INTELLECTUAL PROPERTY: A PROPOSAL FOR THE PUBLIC USE BAR

Ari Ezra Waldman[1]

Abstract

How to draw the line between public and private is a foundational, first-principles question of privacy law, but the answer has implications for intellectual property, as well. Both patent law—through the "public use" bar—and trade secret law—through limited disclosures of confidential information—confront the question of whether legal protection should extend to information previously disclosed to a small group of people. This project, which follows previous scholarship on privacy-as-trust, is one in a series of papers on the effects of defining the boundary between public and non-public information through the lens of social science and, in particular, social network theory and interpersonal concepts of trust among individuals. Patent law's public use bar, relying on a standard of loss of control for determining when a pre-patenting use or disclosure defeats patentability, appears to privilege the confidentiality and control norms of industry while minimizing and ignoring the very different norms and manifestation of confidentiality common to lone entrepreneurs. In so doing, the public use bar has unintended negative effects, including discouraging experimentation and discriminating against inventors without the financial backing of corporate employers. This project proposes a new way of talking about, thinking through, and determining when previous disclosures bar subsequent patentability. In short, I argue that patent and trade secret disclosures in contexts of interpersonal trust retain their legal protection despite any ostensible loss of control or lack of formal confidentiality agreements. This proposal respects social network differences and will advance the goals of patent law and increase access to the innovation economy for all persons.

[1] Associate Professor of Law and Director, Innovation Center for Law and Technology, New York Law School. Ph.D., Columbia, 2015; J.D., Harvard Law School, 2005. This project developed out of a chapter in the author's doctoral dissertation at Columbia University's Department of Sociology. Thanks to Bill McGeveren, John Whealan, Rebecca Tushnet, Gil Eyal, and Jake Sherkow for advice and insight. Thanks to all those participating in the 2015 Works-in-Progress Intellectual Property Conference and the 2015 Intellectual Property Scholars Conference for their feedback. Jeffrey Saavedra is providing essential research assistance.

Introduction

A variety of claims depend on whether information previously disclosed to another is still legally protectable as private. For example, a victim of nonconsensual pornography, commonly known as "revenge porn," may sue for public disclosure of private facts.[2] But the success of her claim hinges on whether she retains a privacy interest in a "selfie" that she may have voluntarily texted to an ex-boyfriend.[3] A Fourth Amendment challenge to the admission of a defendant's cell site data at trial will generally fail because previous disclosure of that data to the phone company extinguishes the defendant's reasonable expectation privacy.[4] And, in certain cases, retention of attorney-client privilege after a disclosure to a third party depends on whether the third party was truly an unrelated member of the public or a close ally in litigation.[5]

The boundary between public and private is a foundational question of privacy law. And, as such, it has engendered myriad answers from privacy scholars.[6] But the question of when information remains legally protectable despite previous disclosure is not the exclusive realm of those writing about privacy; intellectual property lawyers have an interest in this fight, as well. Section 102 of the Patent Act, as amended recently by the America Invents Act (AIA), states that an invention "in public use" or "disclose[d]" or "otherwise available to the public" for more than one year prior to filing an application for the patent will not be considered novel and, thus, not eligible for a patent.[7] And Section 1 of the Uniform Trade Secrets Act, codified as law in 47 states and the District of Columbia,

---

[2] *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 357-59 (2014) (noting the possibility of non-consensual pornography victims using the tort of public disclosure of private facts, but also highlighting the barriers to success for victims using tort law).

[3] *See* Mary Anne Franks, *Combatting Non-Consensual Pornography: A Working Paper* (2014), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2336537.

[4] *See, e.g.*, United States v. Davis, 785 F.3d 498 (11th Cir. 2015); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013).

[5] *See* United States v. Kovel, 296 F.2d 918, 921-2 (2d Cir. 1961) (recognizing that disclosure to a non-lawyer could still permit protection of the privilege in limited circumstances).

[6] Although the full breadth of the privacy literature in this area is too extensive to list here, several works collect and analyze the scholarship well. *See, e.g.*, Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 301, 307-337 (2015); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1099-1126 (2002); Julie Cohen, *Examined Lives: Information privacy and the Subject as Object*, 52 STAN. L. REV. 1373, *et seq.* (2000).

[7] 35 U.S.C. § 102(a)(1). Fortunately, the current § 102(a) closely tracks the language of the pre-AIA § 102(b). Mark A. Lemley, *Does "Public Use" Mean the Same Thing It Did Last Year?*, 93 TEX. L. REV. __ (manuscript at 9) (forthcoming 2015), available at http://papers.ssrn.com/abstract=2394153. Many patent scholars have also proposed new approaches to the public use bar. *See, e.g.*, Katherine White, *A General Rule of Law is Needed to Define Public Use in Patent Cases*, 88 KY. L.J. 423 (2000).

requires trade secrets be "not generally known" and the subject of reasonable efforts to keep them secret.[8] What is a *public* use under the Patent Act and what is not *generally* known in trade secret law depends on drawing the line between public and private, and each regime draws the line differently. This Article bridges a gap between privacy and intellectual property scholarship and proposes a conceptual and practical framework for determining when a previously disclosed invention is still patentable.[9] In short, it depends on social network norms and relationships of trust: when the relationship between the parties is characterized by trust and expectations of confidentiality, information disclosed should remain protected.

Public use case law links publicness with the inventor's loss of control over her invention prior to patenting.[10] In this way, one of the dominant conventional theories of privacy[11]—privacy as the right to control what others know about you—is reflected in patent law's novelty jurisprudence. This theory is an affirmative right located within the individual that embraces principles of autonomy and choice. It separates the private and public worlds with retention and loss of control over information, respectively.

As a means of determining the extent of personal privacy rights, a doctrine based on control and secrecy is problematic. As Dan Solove has argued, its bright-line rule extinguishes our privacy interests when any third party knows something about us, an

---

[8] Uniform Trade Secrets Act (UTSA) § 1(4)(i)-(ii).

[9] Notably, copyright litigation often requires courts to determine whether a given performance, transmission, distribution or display of a copyrighted work was "to the public." 17 U.S.C. § 106. *See, e.g.*, American Broadcasting Company v. Aereo, 134 S. Ct. 2498 (2014). But that determination raises different law and policy questions. Patent law's public use bar and trade secret's limited disclosure rules concern first-person disclosures that could limit future rights; they focus on occasions when the inventor demonstrates her device or when the owner of a trade secret divulges confidential information. Those scenarios are conceptually similar to when an individual discloses personal information to a small group, expecting it to remain within that network. On the other hand, public performance questions like those at issue in *Aereo* are neither based on actions of the copyright owner nor relevant to a potential future limitation on her rights. Therefore, the public versus private distinction in copyright law is omitted from this discussion.

[10] *See infra* notes 21-35 and accompanying text.

[11] Privacy as control is a dominant theory in privacy scholarship. *See, e.g.*, Charles Fried, *Privacy*, 77 YALE L.J. 475, 484 (1968); Jean L. Cohen, *The Necessity of Privacy*, 68 SOC. RESEARCH 318, 319 (2001); JULIE INNESS, PRIVACY, INTIMACY, AND ISOLATION 56-57 (1992); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). Elsewhere, I have argued that although conceptualizations of privacy vary wildly, the conventional wisdom is really two sides of the same coin. For some, the private world represents freedom *from* society; for others, privacy gives us the individual freedom *for* autonomous lives of free choice. All are based on the same respect for the individual as the locus of the privacy right, and all are burdened by limitations: some are overinclusive, while others are underinclusive; some are too elastic, while others are egregiously rigid. *See* Waldman, *supra note* 6, at 307-37.

increasingly common phenomenon in a networked world.[12] In so doing, it allows others to encroach on spheres we would normally consider private.[13] Similarly, as a means of determining the difference between public and non-public uses and disclosures under the Patent Act, privacy as control discourages experimentation and innovation and frustrates the goals of patent law generally. As implemented, the standard is also discriminatory. It privileges wealthy and corporate inventors over other innovators by relying too heavily on executed confidentiality agreements and the confidentiality norms of corporate actors. As a result, by disrespecting how many entrepreneurs commonly interact with others, the public use bar entrenches wealthy interests and excludes other entrepreneurs from the innovation economy.

Relying on research into social networks and interpersonal trust, this Article proposes a new way of talking about, thinking through, and determining when previous disclosures bar subsequent patentability. I argue that disclosures in networks characterized by interpersonal trust retain their privacy interests despite any ostensible loss of control or lack of formal confidentiality agreements. I call this proposal "privacy as trust" and I apply it from the privacy context to the public use bar. Trust, defined as expectations of others' future behavior and incorporating the principles of social network theory, is the defining feature of social interaction.[14] It is arguably the catalyst for an individual's decision to disclose otherwise private information.[15] And because we share when we trust and because trust is a contextual social phenomenon, it makes intuitive sense to distinguish between public and private uses or disclosures along these lines using a totality of the circumstances test.

Applying privacy as trust to the public use context has several advantages: it is egalitarian, flexible, practical, and retains fidelity to the policy objectives of patent law. By respecting the confidentiality norms of different social groups, privacy as trust and its totality of the circumstances test would help rebalance public use jurisprudence among all types of inventors. It is also flexible enough to accommodate myriad different social contexts, many of which are characterized by such strong notions of confidentiality that formal

---

[12] Dan Solove has called this the "secrecy paradigm." DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 42-47, 143-149 (hereafter, "DIGITAL PERSON") (2004).

[13] *Id.* at 42-43, 143.

[14] J. David Lewis & Andrew Weigert, *Trust as a Social Reality*, 63 SOC. FORCES, 967, 969 (1985).

[15] *See* Waldman, *supra* note 6, 342-51; Ari Ezra Waldman, *Data Report: Trust as a Factor in User Motivations to Share Personal Information on Facebook*, DATA PRIVACY PROJECT AT NEW YORK LAW SCHOOL (forthcoming 2015) (presenting quantitative data showing that trust is a key, statistically significant factor in individuals' decision to share personal information on Facebook).

agreements are unnecessary. The standard is also administrable on a case-by-case basis, offering clear opportunities for the admission of evidence of expectations of social network confidentiality alongside myriad other cues of non-public disclosure. And it will advance the policy goals of patent law by protecting inventors' rights, encouraging experimentation, and freeing up public information for future use.

What's more, this proposal is not as radical as it seems. Social network theory and trust are already at play throughout intellectual property law. We see respect for social networks in patent law's enablement requirement, which is defined relative to someone "of ordinary skill in the art" of the invention. Copyright law's originality requirement is genre-specific, recognizing that originality and creativity mean different things for different cultural artifacts. And trademark law accepts that two companies can use similar marks as long their products, marketing channels, and consumer markets remain in separate networks.

Beyond merely incorporating social network theory and recognizing a network-specific reality, trade secret law goes further; it gets us closer to a relationship-oriented, trust-based, network-specific disclosure analysis. Whereas patent law's public use bar determines publicness from the patentee's perspective, asking whether she retained or lost control of her invention, trade secret law shifts the analysis to the nature of the social relationship between the parties. It also takes into account the social context of the disclosure rather than rely almost exclusively on legal formalities. As Sharon Shandeen has shown, this doctrine of "relative secrecy" helps trade secret owners retain legal protection over their confidential business information after limited disclosures.[16] But although we can learn much from trade secrecy's respect for social networks, its lessons are still limited by near exclusive emphasis on corporate actors, norms, and power. Privacy as trust would expand the relationship model to respect the norms of confidentiality of different types of inventors.

This Article proceeds in three parts. Part I surveys and analyzes public use case law and makes two related arguments. First, that privacy as control has so far been the dominant standard for determining when pre-patenting disclosures implicate the "public use" bar. Second, as implemented, the standard discriminates against non-corporate entrepreneurs by privileging the confidentiality norms of corporate actors over the distinct norms and practices of other social networks. This section also criticizes the logical failure of a disclosure standard that ignores the relationships between the parties involved. To resolve that central failure, Part II proposes a new standard. Using social networks theory and social science evidence on

[16] Sharon Shandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 696 (2006).

information flow and interpersonal trust, this Article argues that privacy as trust is a fair and administrable way to draw the line between public and nonpublic disclosures. The doctrine holds that information disclosed in a context of trust, based on network-specific norms of confidentiality, custom, and the entirety of the social context of disclosure, are not public and, thus, still protectable as private. This section concludes by showing the advantages of this proposal. Part III returns to several of the public use cases discussed in Part I, and applies privacy as trust to these real contexts. Sometimes, though not always, results would change under the new standard; in all cases, privacy as trust is fair, egalitarian, and loyal to the goals of patent law. I respond to several anticipated objections and conclude with recommendations for future research.

I. Patent Law's Denial of Social Relationships

To get a patent, your invention must be novel. To be novel, it cannot have been in public use, disclosed, or otherwise available to the public more than one year prior to patenting.[17] If, as several leading patent scholars have argued,[18] the recent America Invents Act amendments do not change the meaning of the novelty requirement, patent law's publicity triggers will continue to be based on either a secrecy paradigm[19] or, in the case of the public use bar, on the extent to which an inventor retains control over her invention during pre-patent use. The purposes of the public use bar are noble ones: to incentivize prompt disclosure, discourage inventors from commercializing their products while keeping prior art out of the public domain, and to give inventors a reasonable amount of time to determine the market for their products.[20]

---

[17] 35 U.S.C. § 102(a).

[18] *See* Lemley, *supra* note 7; Robert P. Merges, *Priority and Novelty Under the AIA*, 27 BERKELEY TECH. L.J. 1023 (2012).

[19] SOLOVE, DIGITAL PERSON, *supra* note 12, at 42-47 (introducing, describing, and ultimately critiquing the "secrecy paradigm" in privacy jurisprudence). The "secrecy paradigm" is evident in the Federal Circuit's interpretation of Section 102(a) of the Patent Act of 1952 in that anything not secret is public. As the court stated recently in *In re Enhanced Security Research, LLC*, 739 F.3d 1347 (Fed. Cir. 2014), § 102 has always been interpreted "broadly." *Id.* at 1354. "[E]ven relatively obscure documents," like a single copy of a graduate thesis buried in a German university library, "qualify as prior art so long as the public has a means of accessing them." *Id.* (citing In re Hall, 781 F.2d 897, 899, 900 (Fed. Cir. 1986)). The Federal Circuit made a similar conclusion in *W.L. Gore & Assocs., Inc. v. Garlock*, 721 F.2d 1540 (Fed. Cir. 1983), where it found that process for rapidly stretching TEFLON without it breaking was publicly used even though it was only used inside Gore's shop. *Id.* at 1549. And, of course, the famous and oft-cited *Egbert v. Lipmann*, 104 U.S. 333 (1881), which held that a woman was publicly using a corset invented by her fiancé even though she was wearing the only prototype under her clothes, is a paradigmatic example of the secrecy paradigm, as well.

[20] Tone Bros. v. Sysco Corp., 28 F.3d 1192, 1198 (Fed. Cir. 1994). *See also e.g.*, Nancy S. Paik, *Implied Professional Obligation of Confidentiality Sufficient To Overcome Public Use Defense to a Claim of Patent Infringement?* Bernhardt v. Collezione—*The*

In practice, however, the public use rule—that retention of control, based ostensibly on a totality of the circumstances test, is incompatible with public use—generally overemphasizes the importance of formal confidentiality agreements and commonly ignores the confidentiality norms inherent in non-corporate and non-contractual social relationships. As such, the public use bar privileges corporate, wealthy, and established inventors for whom contracts and nondisclosure agreements come easily. And it makes it difficult for other types of entrepreneurs to test and market their inventions. In this section, I summarize the law of public use, show how similar it is to one of the dominant theories of privacy, and then illustrate its uneven application using a series of illustrative public use case studies. I conclude with a short discussion of how current application of the public use bar tends to institutionalize corporate privilege and limits entrepreneurs' access to the innovation economy.

A. The Public Use Bar and Privacy as Control

Federal Circuit case law states that lack of control is the shibboleth of public use: a public use occurs when an inventor allows others to use her invention without retaining control over the device.[21] In a nod to the connection between public use and privacy, the Federal Circuit has noted that control depends on whether the inventor retained a "legitimate expectation of privacy and of confidentiality."[22] Like privacy questions, then, public use claims require judges to determine when an expectation of privacy exists. And like an individual's expectations of privacy, whether an inventor retained control over her invention is supposed to be based on a variety of non-determinative factors. In the public use context, those factors include: the nature of the activity that the inventor engaged in in public, the public's access to and knowledge of the use, whether the inventor imposed confidentiality obligations on those present,[23] and evidence of experimentation.[24] The one factor—the presence of confidentiality or secrecy obligations—ostensibly focused on the relationship between the inventor and the public is supposed to be

---

Federal Circuit Court of Appeals' Surprising Recent Announcement on the Public Use Bar, 4 CHI.-KENT J. INTELL. PROP. 332, 333-34 (2005).

[21] Moleculon Research Corp. v. CBS, Inc., 793 F.2d 1261, 1266 (Fed. Cir. 1986) (nonpublic use because the inventor had at all times "retained control" over the device during pre-patenting demonstrations).

[22] Dey, L.P. v. Sunovision Pharm., Inc., 715 F.3d 1351, 1356 (Fed. Cir. 2013) (citing Netscape Commn's Corp. v. Konrad, 295 F.3d 1315, 1321 (Fed. Cir. 2002)).

[23] Bernhardt, L.L.C. v. Collezione Europa USA, Inc., 386 F.3d 1371, 1379 (Fed. Cir. 2004).

[24] Atlanta Attachment Co. v. Leggett & Platt, Inc., 516 F.3d 1361, 1368-69 (Fed. Cir. 2008) (Prost, J., concurring).

flexible: a formal nondisclosure agreement is not required.[25] As we shall see, that flexibility is unevenly applied.

Experimental use, which is supposed to negate a finding of public use, is also determined via the totality of the circumstances: "the number of prototypes and duration of testing, whether records or progress reports were made concerning the testing, the existence of a secrecy agreement between the patentee and the party performing the testing, whether the patentee received compensation for the use of the invention, and the extent of control the inventor maintained over the testing."[26] That the multifactor tests overlap is telling. Public use is most appropriately determined in context on a case-by-case basis because each disclosure occurs in a unique set of circumstances.

But at the core of public use law is the control the inventor retains over her invention. And an inventor's choice to give up control is the salient factor in nudging a court toward a finding of public use. The Supreme Court made this clear in 1877. In *City of Elizabeth v. American Nicholson Pavement Co.*,[27] the Court stated that as long as an inventor "does not voluntarily allow others to make [the invention] and use it, and so long as it is not on sale for general use, he keeps the invention under his own control, and does not lose his title to a patent."[28] This cause-and-effect relationship between voluntarily disclosure and erosion of control is the hallmark of modern public use law, as well.[29]

In *Lough v. Brunswick, Corp.*,[30] for example, the Federal Circuit invalidated a patent for boat motor seals because the inventor gave away his invention, installed it on another's boat, and failed to keep track of the test boat's operation with the installed prototype.[31] In *Beachcombers International, Inc. v. WildeWood Creative Products*,[32] a designer lost her patent for a new kaleidoscope because she chose to demonstrate the invention for party guests and allowed them to handle and use it.[33] And in *Baxter International v. Cobe Laboratories*,[34] an inventor lost control of his invention (and thus lost his patent) not

[25] Moleculon Research Corp. v. CBS, Inc., 793 F.2d 1261, 1266 (Fed. Cir. 1986).

[26] Lough v. Brunswick Corp., 86 F.3d 1113, 1120 (Fed. Cir. 1996) (*citing* TP Labs. v. Professional Positioners, Inc., 724 F.2d 965, 971-72 (1984)).

[27] 97 U.S. 126 (1877).

[28] *Id.* at 135.

[29] *Elizabeth* has been cited in 423 subsequent cases for the proposition that an inventor's voluntary giving up of her device constitutes a loss of control for the purposes of a public use finding. Though technically an experimental use case, *Elizabeth*'s rule has been applied to public use, generally.

[30] 86 F.3d 1113 (Fed. Cir. 1996).

[31] *Id.* at 1121.

[32] 31 F.3d 1154 (Fed. Cir. 1994).

[33] *Id.* at 1159-60.

[34] 793 F.2d 1261 (Fed. Cir. 1986).

only because he demonstrated his new centrifuge for others, but also because he allowed a free flow of bodies through his lab that housed the device.[35] In these and many other cases, the Federal Circuit took away patents because inventors had voluntarily given over their inventions to others and, in so doing, made the decision to give up control over their devices.

In this way, patent law's public use bar reflects one of the dominant conceptualizations of privacy: privacy as choice and control. This is the theory that a right to privacy means having the right to control personal information and the freedom to decide to share it with some and not others. This paradigm is pervasive, evident in leading works of privacy scholarship and a multitude of privacy cases. And the language scholars and judges use to describe privacy is reminiscent of the Federal Circuit's discussion of public use and control.

Privacy as control scholars could just as easily be speaking about individuals concerned about their privacy as inventors disclosing their devices. For instance, Jean Cohen has argued that privacy is the right "to choose whether, when, and with whom" to share intimate information.[36] Alan Westin suggests that privacy "is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[37] It is, to Julie Inness, the idea that an individual has "control over a realm of intimacy"[38] and, to Jonathan Zittrain, control over our information, in general.[39] For the philosopher Steve Matthews, exercising privacy is making the choice to "control" and "manage" the boundary between ourselves and others.[40] The common denominator in all these descriptions is free choice and control, and it is the same dynamic at play in cases like *Elizabeth*, *Lough*, *Beachcombers*, and *Baxter*.

Privacy as control is also evident in the current interpretation of the tort of public disclosure of private facts.[41] Here, too, the comparison to public use analysis is striking. Although the tort's often uneven application has spawned much debate and

---

[35] *Id.* at 1058-59.

[36] Jean L. Cohen, *The Necessity of Privacy*, 68 SOC. RES. 318, 319 (2001)

[37] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

[38] JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992).

[39] Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1203 (2000) ("In my view, there is a profound relationship between those who wish to protect intellectual property and those who wish to protect privacy.").

[40] Steve Matthews, *Anonymity and the Social Self*, 47 AM. PHIL. Q. 351, 351 (2010).

[41] Restatement (Second) of Torts § 652D (1992).

scholarship,[42] the general rule reflects privacy as control: an individual tends to lose control and, thus, a privacy interest, in information once an she has voluntarily divulged it to another or once the information is already publicly available.[43] Like Oliver Sipple, who could not prevent the media from disclosing his sexual orientation after he had already disclosed it to friends in San Francisco,[44] and like Ralph Nader, who could not prevent General Motors from gathering personal information already known to others,[45] the inventors in *Lough*, *Beachcombers*, and *Baxter* could not put the cat back in the bag. Their inventions, either from voluntary disclosures (*Lough* and *Beachcombers*)[46] or public availability (*Baxter*)[47], were already out of their control and known and used by others.

B. The Uneven Application of the Public Use Bar

It is evident, then, that the law of public use reflects the dynamics of privacy as control. That itself is problematic because it creates the potential for what Dan Solove has called a "secrecy paradigm" to govern what should be a more flexible, case-by-case standard. In privacy law, the secrecy paradigm refers to the erroneous conflation of privacy and secrecy: it creates a bright line rule that something is private if it is secret, but if it is known to even one other person, it is no longer secret and, thus, not protectable as private.[48] It is at play all over the privacy spectrum, from tort law[49] to the Fourth Amendment.[50]

---

[42] *See, e.g.*, Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005); Waldman, *supra* note 6.

[43] *See, e.g.*, Killelea v. Sears, Roebuck & Co., 499 N.E.2d 1291, 1295 (Ohio Ct. App. 1985) ("There is no liability when the defendant merely gives further publicity to information about the plaintiff that … the plaintiff leaves open to the public."); Sipple v. Chronicle Publ'g Co., 210 Cal. Rptr. 665 (Cal. Ct. App. 1984) (disclosure of Sipple's sexual orientation to a group of people extinguished his privacy interests in the information upon subsequent disclosure to the broader public); Nader v. General Motors, Corp., 255 N.E.2d 765 (N.Y. 1970) ("Information about the plaintiff which was already known to others could hardly be regarded as private."). *But see, e.g.*, Y.G. v. Jewish Hospital, 795 S.W.2d 488 (Mo. Ct. App. 1990) (voluntarily attending a social gathering at a hospital with media in attendance did not vitiate privacy interest in family's decision to use in vitro fertilization).

[44] Sipple, 210 Cal. Rptr. at 668-69.

[45] Nader, 255 N.E.2d at 770.

[46] Lough, 86 F.3d at 1121 ("He provided the seal assemblies to friends"); Beachcombers, 31 F.3d at 1159 (voluntarily giving her kaleidoscope to party guests).

[47] Baxter, 88 F.3d at 1056, 1058 (inventor showed others how the centrifuge worked and permitted free flow through his lab, allowing all who passed to see the device).

[48] SOLOVE, DIGITAL PERSON, *supra* note 12, at 42-47, 143-149.

[49] *See, e.g.*, *supra* note 43.

[50] *See, e.g.*, United States v. Miller, 425 U.S. 435 (1976) (no reasonable expectation of privacy in bank records); Smith v. Maryland, 442 U.S. 735 (1979) (no reasonable expectation of privacy in numbers captured by pen register). The Third

It helps explain several public use cases, as well. In *Lough*, the inventor showed his device to five friends, who used it on their boats.[51] In *JumpSport v. Jumpking*,[52] an inventor allowed a few neighbors to use his backyard trampoline outfitted with safety enclosures.[53] And in the classic case of *Egbert v. Lippmann*,[54] the Supreme Court stated that an "intimate friend" wearing a corset under her clothes constituted public use: "If an inventor, having made his device, gives or sells it to another, to be used by the donee or vendee, without limitation or restriction, or injunction of secrecy, and it is so used, such use is public, even though the use and knowledge of the use may be confused to one person."[55] The secrecy paradigm may have the benefit of clarity, but it imposes a harsh bright line rule where case-by-case precision may be more appropriate.

The secrecy paradigm alone, however, fails to explain the majority of public use cases. As applied, public use law is less indiscriminate blunt axe than discriminatory scalpel. Sometimes, the Federal Circuit applies its rule that confidentiality agreements are just one factor to consider; elsewhere, nondisclosure agreements are treated as essential. And sometimes, norms of confidentiality are respected; at other times, they are ignored. The result sounds like a confusing muddle, but one distinct pattern emerges: corporate inventors tend to win their public use cases; solo entrepreneurs tend to lose.[56]

Party Doctrine, spawned by *Miller*, *Smith*, and their progeny, reflects the secrecy paradigm. The doctrine states that individuals cannot have a legitimate expectation of privacy in information in the hands of third parties. It is the subject of great criticism in the legal academy. *See* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 752-53 (2005). *But see generally* Orin Kerr, *A Case for the Third Party Doctrine*, 107 MICH. L. REV. 561 (2009).

[51] Lough, 86 F.3d at 1121.

[52] 191 Fed. Appx. 926 (Fed. Cir. 2006).

[53] JumpSport, Inc. v. Jumpking, Inc., No. C 01–4986 (N.D. Cal. June 2, 2003) (June 2, 2003 Order) ("several neighbors").

[54] 104 U.S. 333 (1881).

[55] *Id.* at 335-36.

[56] This Article uses the hierarchical clustering technique to distinguish between two clusters of inventors: (A) those that are supported by large corporate structures, and (B) those that invent in their spare time or without corporate resources. Cluster analysis is a method for grouping objects together in groups (clusters) based on their similarities across a series of variables. *See* Kenneth D. Bailey, *Cluster Analysis*, 6 SOC. METHODOLOGY 59, 61 (1975). It is a way of drawing boundaries around things that generally behave similarly and, as such, it is widely applied in the social sciences, data mining, and even biology. *See* BRIAN S. EVERITT, CLUSTER ANALYSIS (2011); ANDREW R. WEBB, STATISTICAL PATTERN RECOGNITION (2002); TERRY SPEED, STATISTICAL ANALYSIS OF GENE EXPRESSION MICROARRAY DATA (2003). For example, a sociologist may find that several characteristics (independent variables like age, location, and sex) help explain a given behavior (some dependent variable). Male urban youths ages 13-18

Several case studies, all of which are summarized in Figure I, illustrate that argument: corporate inventors often do not need nondisclosure agreements, lone entrepreneurs do. And corporate norms of confidentiality—among employees and between companies in arm's length dealing—are usually respected, whereas the more informal, but no less powerful confidentiality norms of social friends and other interpersonal networks are often ignored. This is another effect of using privacy as control in the public use context: because it offers no clear guidelines on what happens to information after it is no longer a literal secret, it allows judges to privilege certain forms of control over others.

---

tend to behave similarly in one respect, while female suburban youths ages 13-18 behave similar to each other. The two groups can create two or more clusters, depending on the method of analysis and research goal. Cluster analysis does not suggest that all data points in a given cluster are identical or always behave similarly. Rather, they are similar across a closed subset of variables; they may behave differently across a different set of independent variables or relative to different dependent variables. There are myriad methods for determining clusters. Hierarchical clustering is based on the idea that objects are more related to objects nearby than objects far away. It employs algorithmic and graphical analysis to determine clusters. *See* Brian S. Everitt, *Unresolved Problems in Cluster Analysis*, 35 BIOMETRICS 169, 170-77 (1979); Baibing Li, *A New Approach to Cluster Analysis: The Clustering-Function-Based Method*, 69 J. ROYAL STAT. SOC. 457, 457 (2006). For this Article, I plotted, in two-dimensional space, the relationship between inventor identity defined by connection to and invention support by an employer and public use result in the cases in Figure I. Relative size and strength of employer was based on available corporate revenue data from Bloomberg or Hoover.com. Cluster A consists of engineers, programmers, and other inventors employed by large corporations who invent devices in course of their employment and with the institutional support of their employers. Cluster A includes experts as Xerox, biochemists at large pharmaceutical companies, and mechanical engineers at Honeywell, for example. Cluster B consists of students, hobbyists, and experts inventing in their spare time. The members of these groups were similar to each other on the relevant variables. Three cases were eliminated from consideration because, given the facts, clustering would have been arbitrary. Subsequent research could probe whether some small- or medium-sized businesses are treated fairly in the public use context.

Case	Inventor Cluster (A=Corp Inventor; B=Solo Entrepreneur)	Disclosure Event	Signed secrecy or confidentiality agreement?	Public Use?
Xerox v. 3Com	A (Inventor in course of employment for large company)	To chair of conference	No	No
Pronova BioPharma Norge AS v. Teva Pharmaceuticals USA	A (For large chemical co.)	Samples sent to dr. for testing	No	Yes
Bernhardt LLC v. Collezione Europea USA	A (President of one of the largest family-run furniture co's in US)	Display at industry trade show	No	No
Dey LP v. Sunovion Pharmaceuticals	A (Big Pharma)	Clinical trials	Yes and No	No
Lough v. Brunswick Corp.	B (Repairman)	Installed on friends' boats	No	Yes
MIT v. Harman Int'l Industries	B (Students)	Testing and demos	No	Maybe
Minnesota Mining & Mfg. v. Appleton Papers	A (Company president)	Distributed to 1000s of employees	No	Yes
Beachcombers v. WildeWood Creative Products	B (Part-time inventor)	Demo and use for 20-30 invited guests at inventor's home	No	Yes
Baxter In'tl v. Cobe Laboratories	B (Researcher)	Demos and free flow through lab	No	Yes
Moleculon Research Corp. v. CBS, Inc.	A (Graduate student, but large company defending validity)	Shown to friends, roommate, chemistry department colleagues, employer (who sent it to 50-60 toy companies)	No	No
American Seating v. USSC Group	A (Spare-time inventor, but large company defending validity)	Demos to friends and colleagues for feedback	No	No
In re Hamilton	B (Lone inventor)	Test runs	No	Yes
NRDC v. Varian Associates	B (Graduate student)	Adviser disclosed to individual at conference	No	Yes
Delano Farms v. California Table Grape Commission	A (Owners of large grape growing company)	Distributed grape varieties to friends/family	No	No
Invitrogen v. Biocrest Mfg.	A (For large company)	Used internally in co.	No	No

Case	Inventor Cluster (A=Corp Inventor; B=Solo Entrepreneur)	Disclosure Event	Signed secrecy or confidentiality agreement?	Public Use?
Netscape Communications v. Konrad	B (Staff scientist, part-time inventor)	Shown to colleague	No	Yes
Motionless Keyboard v. Microsoft	B (Part-time inventor)	Shown to friends and potential investor	Yes	No
Petrolite Chemicals v. Baker Hughes	A (For large chemical company)	Testing	No	Yes
Honeywell Int'l v. Universal Avionics Systems	A (For large aviation company)	Demos of plane with reporter on board	No	No
Allied Colloids v. American Cyanamid	A (Large chemical company)	Testing process to win back commercial contract with city	No	No
Eli Lilly v. Zenith Goldline Pharmaceuticals	A (Big Pharma)	Open clinical trials	No	No
JumpSport v. Jumpking	B (Hobbyist inventor)	Used by several neighbors in inventor's backyard	No	Yes
Manville Sales v. Paramount Systems	A (Researcher in course of employment for large co.)	Drawings distributed and invention testing in pilot	Yes	No
New Railhead Mfg. v. Vermeer Mfg.	A (Company president)	Used by acquaintance at public job site	No	Yes
Eolas Technologies v. Microsoft	B (Student)	Demos to 2 Sun Microsystems employees	No	Yes

Figure I

Public use bar cases comparing type of inventor and nondisclosure agreements with result.

1. The Privileged Position of the Corporate Inventor: Confidentiality Agreements

Courts tend to give corporate inventors the benefit of the doubt on their public use defenses. When the disclosing party is a corporate inventor, rules are generally flexible, seemingly applied with the goal of protecting the corporation's patents. Nondisclosure agreements are rarely required and informal industry norms of confidentiality are often respected.

Of the 25 public use cases included in this analysis, nine feature Cluster A (corporate) defendants that won findings of nonpublic use despite disclosures occurring without formal confidentiality agreements.[57] At the same time, ten Cluster B (solo entrepreneur) defendants faced the opposite result—no confidentiality agreement and a finding of public use.[58] But beyond just the results, courts' perspectives on the importance of formal confidentiality agreements also change based on the type of public use defendant. For corporate inventors, rules are flexible; for lone entrepreneurs, confidentiality agreements have heightened importance. In *Dey L.P. v. Sunovion Pharmaceuticals*,[59] a case involving two large pharmaceutical companies, the Federal Circuit determined that use of COPD medication in clinical trials did not constitute public use even though the patients involved never signed confidentiality agreements.[60] The court recognized that clinical trial patients customarily do not sign confidentiality agreements; to require one in this case would ignore the contextual factors that implied a baseline of confidentiality regardless of any agreement.[61] To reinforce that flexible approach, the court even admonished the district court below for its overly formalistic reliance on executed agreements.[62] And in *Bernhardt v. Collezione Europea USA*,[63] where one of the largest family-owned furniture companies in the United States displayed patented material at an industry trade show that did not require signed confidentiality agreements,[64] the court noted that a formal secrecy agreement "is just one factor to consider" and immediately reframed the analysis as a totality of the circumstances test for inventor control in context.[65]

---

[57] *See* Xerox v. 3Com, 26 F. Supp. 2d 492 (Fed. Cir. 1998); Bernhardt v. Collezione Europa USA, 386 F.3d 1371 (Fed. Cir. 2004); Dey v. Sunovion Pharm., 715 F.3d 1351 (Fed. Cir. 2013); American Seating v. USSC Group, 514 F.3d 1262 (Fed. Cir. 2008); Delano Farms v. California Table Grape Cmm'n, 778 F.3d 1243 (Fed. Cir. 2015); Invitrogen v. Biocrest Mfg., 424 F.3d 1374 (Fed. Cir. 2005); Honeywell Int'l v. Universal Avionics Sys., 448 F.3d 982 (Fed. Cir. 2007); Eli Lily v. Zenith Goldline Pharm., 471 F.3d 1369 (Fed. Cir. 2006).

[58] *See* Lough v. Brunswick Corp., 86 F.3d 1113 (Fed. Cir. 1996); Mass. Inst. of Tech. v. Harman Int'l Indus., 584 F. Supp. 2d 297 (D. Mass. 2008); Beachcombers v. WildeWood Creative Pros., 31 F.3d 1154 (Fed. Cir. 1994); Baxter Int'l v. Cobe Labs., 88 F.3d 1054 (Fed. Cir. 1996); In re Hamilton, 882 F.2d 1576 (Fed. Cir. 1989); Nat'l Resources Defense Council v. Varian Assoc., 17 F.3d 1444 (Fed. Cir. 1994); Motionless Keyboard v. Microsoft, 486 F.3d 1376 (Fed. Cir. 2007); JumpSport v. Jumpking, 191 Fed. Appx. 926 (Fed. Cir. 2006); Netscape Comm's v. Konrad, 295 F.3d 1315 (Fed. Cir. 2002); Eolas Tech. v. Microsoft, 399 F.3d 1325 (Fed. Cir. 2005).

[59] 715 F.3d 1351 (Fed. Cir. 2013).

[60] *Id.* at 1354.

[61] *Id.* at 1357-58.

[62] *Id.* at 1357.

[63] 386 F.3d 1371 (Fed. Cir. 2004)

[64] *Id.* at 1374.

[65] *Id.* at 1379-80.

But courts are rarely so charitable and flexible in cases involving Cluster B (solo entrepreneur) defendants. In *Baxter*, for example, the Federal Circuit found that the use of a centrifuge by an NIH researcher in his personal laboratory constituted disqualifying public use because he maintained no control over the device. The most important factor leaning against control seemed to be the fact that the inventor demonstrated the technology to colleagues without a confidentiality agreement or any indication that it should be kept secret.[66] In *Lough*, a corrosion-proof seal for stern drives was tested on boats belonging to several of the inventor's friends and colleagues.[67] The court determined that the use was public because the inventor lacked any control over the seals: he asked for no follow up, did not supervise their use, and never asked his friends to sign confidentiality agreements.[68] And in *Massachusetts Institute of Technology v. Harman International Industries*,[69] inventors used their friends to test a car navigation system, but never required confidentiality agreements from them or corporate sponsors.[70] In each of these cases, the lack of a confidentiality agreement between the parties, though ostensibly only one of many factors to consider, was always among the most important.

The narrative in *Beachcombers v. WildeWood Creative Products*[71] makes the point even more clear. In that case, the designer and developer of an improved kaleidoscope wanted to solicit feedback on the design from her friends and colleagues. She invited twenty to thirty of them over to her house for a demonstration and, without asking them to sign a confidentiality agreement, allowed her guests to handle the invention.[72] The situation had all the indicia of a controlled social event: an invite-only guest list consisting of friends and colleagues who were invited for the purposes of testing, experimentation, and feedback. The only thing missing was a formal secrecy agreement. Without it, though, the use was considered sufficiently public because the developer could not control what her guests did with kaleidoscope either at the party or what they did with the information they learned after they left.

---

[66] Baxter, 88 F.3d at 1058-59 (the inventor's "lack of effort to maintain the centrifuge as confidential coupled with the free flow [of people] into his laboratory of people, including visitors to NIH, who observed the centrifuge in operation and who were under no duty of confidentiality," necessitated a finding of "public use.")

[67] Lough, 86 F.3d at 1116.

[68] *Id.* at 1120, 1121. "The last factor of control is critically important." *Id.* at 1120.

[69] 584 F. Supp. 2d 297 (D. Mass. 2008).

[70] *Id.* at 303-4.

[71] 31 F.3d 1154 (Fed. Cir. 1994).

[72] Beachcombers, 31 F.3d at 1159-60 (the inventor "personally demonstrated the device to some of the guests for the purpose of getting feedback on the device; … she made no efforts to conceal the device or keep anything about it secret.").

The correlation may not be perfect: there are several examples listed in Figure I where Cluster A defendants lose their public use cases in part because they failed to secure confidentiality agreements. But, in this case, the exceptions help prove the rule. Like those involving Cluster B defendants above, the opinions in these cases elevate formal secrecy agreements to almost determinative status. In *Pronova Biopharma Norge AS v. Teva Pharmaceuticals*,[73] for example, where a pharmaceutical company sent drug samples to an outside doctor for testing,[74] the court's holding highlighted the central importance of a confidentiality agreement, concluding the public use happened when samples were sent "with no confidentiality restrictions."[75] *Pronova* and cases like *Minnesota Mining and Manufacturing v. Appleton Papers*,[76] *Petrolite v. Baker Hughes*,[77] and *New Railhead Manufacturing v. Vermeer Manufacturing*[78] may not rest exclusively on the lack of formal confidentiality agreements. But the pattern is unmistakable: a nondisclosure contract is, in practice, more important than the black letter law would suggest.[79] This is a boon to corporate inventors even when they lose because, as compared to solo entrepreneurs, part-time developers, and hobbyists, corporate inventors have the leverage and power to insist on confidentiality agreements from their business partners and the money to pay lawyers to draft them.[80]

2. The Privileged Position of the Corporate Inventor: Norms of Confidentiality

---

[73] 549 Fed. Appx. 934 (Fed. Cir. 2013).

[74] *Id.* at 942.

[75] *Id.* at 939.

[76] 35 F. Supp. 2d 1138, (D. Minn. 1999) ("No 3M employee was asked to sign a secrecy agreement before using them. And 3M announced no company-wide policy regarding [the invention's] use or circulation.").

[77] 96 F.3d 1423, 1428 (Fed. Cir. 1996) ("Moreover, there was no evidence that Quaker had entered into any secrecy agreement with Sohio …").

[78] 298 F.3d 1290 (Fed. Cir. 2002).

[79] Moleculon, 793 F.2d at 1266 (a formal confidentiality agreement is supposed to be just one of many nondeterminative factors).

[80] *See* Kenneth M. Casebeer, *Supreme Court Without A Clue: 14 Penn Plaza LLC v. Pyett and the System of Collective Action and Collective Bargaining Established by the National Labor Relations Act*, 65 U. Miami L. Rev. 1063, 1066-67 (2011) (unequal bargaining power between corporations and individuals) (quoting NLRB v. Jones & Laughlin Steel Co., 301 U.S. 1, 33 (1937) ("Thus, in its present application, the statute goes no further than to safeguard the right of employees to self-organization and to select representatives of their own choosing for collective bargaining or other mutual protection without restraint or coercion by their employer. That is a fundamental right."). *See also* Postal Instant Press, Inc. v. Sealy, 43 Cal. App. 4th 1704, 1715-17 (Cal. Ct. App. 1996) (noting inequality of bargaining power between small businesses and large corporations, and acknowledging that "[b]efore the [franchise] relationship is established, abuse is threatened by the franchisor's use of contracts of adhesion presented on a take-it-or-leave-it basis" (internal citations and quotations omitted)).

Corporate privilege in public use law extends beyond a more flexible approach to formal confidentiality agreements. Indeed, the reason why so many Cluster A defendants that fail to secure secrecy commitments win their public use cases is because courts are willing to fill the gap left by a contract with industry norms and customs of confidentiality. They almost never do the same for Cluster B (solo entrepreneur) inventors. The unequal application is two steps back from what would have otherwise been a step forward toward a flexible, social network-oriented approach to public use.

A comparison of two cases—*Bernhardt* and *Beachcombers*—puts this corporate privilege in relief. Neither case featured signed confidentiality agreements, yet Bernhardt won its case, whereas the inventor in *Beachcombers* did not. Bernhardt owned several design patents for furniture,[81] all of which were displayed in their entirety at an exhibition for industry in advance of a large annual trade show. The exhibition was by invitation only, and entry required identification at several points. Bernhardt representatives were also available to escort attendees around and answer questions.[82] Attendees included 69 of Bernhardt's customers and newspaper reporters from "Furniture Today."[83] For the Federal Circuit, the lack of confidentiality agreements, the arguable commercial motive for inviting customers, and the presence of reporters did not make Bernhardt's disclosure of its designs public. Rather, the entirety of the social context of disclosure suggested that norms of confidentiality were in place. The court's conclusion is worth quoting in full:

> While it is clear that [exhibition] attendees were not required to sign confidentiality agreements, … in the circumstances of this case, confidentiality agreements were unnecessary. At trial, Bernhardt presented the testimony … that although no confidentiality agreement was provided to Pre–Market attendees, "[i]t's pretty well understood that confidentiality applies to premarket [sic]." … Pre–Market attendees have an incentive not to divulge Bernhardt's designs[] because they would not be able to participate if they divulged the Pre–Market designs. … Pre–Market was not open to the public, that the identification of attendees was checked against a list of authorized names both by building security and later at a reception desk near the showroom, that attendees were escorted through the showroom, and that attendees were not permitted to make written notes or take photographs inside the showroom.[84]

[81] Bernhardt, 386 F.3d at 1373.
[82] *Id.* at 1374.
[83] *Id.* at 1379.
[84] *Id.* at 1381.

The evidence of industry confidentiality norms and expectations—that it is "pretty well understood that confidentiality applies to" the exhibition—came from Bernhardt's general manager.[85] The court did what black letter public use law tells it to do: look at the entirety of the social context of a given disclosure and respect the norms of confidentiality emanating from that context.

The Federal Circuit changes its tune when the inventor is a solo entrepreneur. In *Beachcombers*, for example, the designer of a new kaleidoscope disclosed her design in a context at least comparable, if not more private, to the exhibition in *Bernhardt*. She hosted 20-30 friends and colleagues at an invite-only cocktail gathering at her home, demonstrated the kaleidoscope and its unique characteristics, and asked for feedback. No members of the press were present. Nor were customers invited; the inventor had no customers.[86] Despite the contextual evidence of implied confidentiality and privacy—an invite-only social gathering at a private home with testimony from the inventor that the purpose of the event was experimental—the court concluded that the demonstrations constituted invalidating public use based on testimony from one of the guests, contradicted by the inventor, that confidentiality was not implied.[87] In other words, the court was comfortable with ignoring social norms and elevating the importance of a confidentiality agreement when the inventor was creating in her spare time.

If the disparate treatment of corporate and solo inventors is insufficiently clear from *Bernhardt* and *Beachcombers*, the contrast between *Xerox v. 3Com*[88] and *NRDC v. Varian Associates*[89] is even starker. In *Xerox*, a Cluster A case, a company employee developed, in the course of his employment, a technique for more efficient computer recognition of handwriting.[90] The alleged invalidating public use was the inventor's submission of a videotape of himself demonstrating the invention to chairpersons of an industry conference at which he wanted to present. No confidentiality agreement accompanied the videotape.[91] But the court said this was not public use because industry norms said otherwise: "[a]s a matter of formal policy and procedure as well as professional courtesy and practice, [the conference] review committees treat every submission confidentially."[92] There may have been no binding secrecy agreement,

[85] *Id.*
[86] Beachcombers, 31 F.3d at 1159-60.
[87] *Id.* at 1160.
[88] 26 F. Supp. 2d 492 (W.D.N.Y. 1998).
[89] 17 F.3d 1444 (Fed. Cir. 1994).
[90] Xerox, 26 F. Supp. 2d at 492-93.
[91] *Id.* at 493.
[92] *Id.* at 496.

the court noted, but conference organizers were "under a professional ethical obligation" to maintain confidentiality.[93]

Such norms were ignored in *NRDC*. That case involved a graduate student who invented a method for improving nuclear magnetic resonance sample analysis,[94] the "essence" of which was disclosed by the student's adviser to a long-standing friend at a scientific conference.[95] Admittedly, there may be a difference between disclosure to a conference organizer and an attendee, but the court in *NRDC* emphasized the lack of a confidentiality agreement and the conference goal of encouraging open dialogue rather than the norms of confidentiality inherent in friendship and at academic conferences.[96] The former set of considerations went unmentioned in *Xerox*, highlighting both the contrasting result and perspectives and language that appear to differ based on the category of the inventor.

C. Implications of Uneven Application of the Public Use Bar

That courts tend to treat corporate inventors and solo entrepreneurs differently is itself a concern. Our laws, in general, and intellectual property laws, in particular, should be applied dispassionately, evenly, and absent discrimination. There are three additional implications of public use law's privileged treatment of corporate inventors, two of which are practical and one is theoretical. The remainder of this Article is an attempt to propose a new solution that responds to all three concerns.

First, the unequal treatment directly increases barriers to entry into the innovation economy for a wide swath of the inventing class by making patent defense harder and more expensive. Obtaining a patent is already an expensive ordeal.[97] But the evidence suggests that a solo entrepreneur's patent is less secure than a corporate inventor's, thus building greater costs into the patent process from the likelihood of future litigation.[98] Litigation increases costs and decreases the net

[93] *Id.*

[94] NRDC, 17 F.3d at *1.

[95] *Id.* at *3.

[96] *Id.*

[97] David Fagundes & Jonathan S. Masur, *Costly Intellectual Property*, 65 VAND. L. REV. 677, 685, 690 (2012). The average patent will cost the applicant approximately $22,000 to successfully prosecute, *id.* at 690, although this number may be conservative, with some costs reaching $30,000. *Id.* at 690 n. 39. Notably, these estimates do not include the potentially devastating effect of a patent being declared invalid.

[98] *See, e.g.*, Alan Ratliff, Damages, Presentation at AIPLA 2007 Annual Meeting at 4 (Oct. 18, 2007), available at http://www.aipla.org/Content/ContentGroups/Speaker_Papers/Annual_Meeting_Speaker_ Papers/200717/Ratliff-paper.pdf ("According to the AIPLA, the cost of large case patent litigation through trial has increased steadily from over $3 to about $5 million per party …"); Posting of David Schwartz, *Claim Construction Reversal Rates I - Overall Reversal Rates*, to Patently-O Patent Law Blog, http://www.patentlyo.com/patent/2008/02/claim-construct.html (Feb. 27, 2008,

present value of a patent, and uncertainty in litigation outcome, evidenced by courts' uneven and sometimes haphazard application of public use, increases costs exponentially.[99] That they are more likely to fail to protect their patents may also discourage entrepreneurs from entering the patent process, opting for trade secrecy[100] or declining to innovate in the first place. In either case, society at large is worse off as knowledge is either silenced or kept under seal.

Second, the pattern of favoring corporate inventors entrenches an already unequal and strikingly homogenous patent landscape. According to the Patent and Trademark Office (PTO), the top 100 patentees each year are large corporations,[101] which, although not itself evidence of inequality—large corporations with many employees likely have more inventions—feeds a larger narrative of entrenched privilege. For example, women remain a distinct minority among science and technology graduates[102] employed in inventor roles at large corporations.[103] Corporate domination of the patent world, therefore, marginalizes their and other minorities' contributions to the innovation economy.[104] A recent study of 4.6

11:00 EST) (tabulating claim construction reversal rates as high as 43.5%); *Inventive Warfare*, THE ECONOMIST, Aug. 20, 2011, at http://www.economist.com/node/21526385; James Bessen & Michael J. Meurer, *The Direct Costs from NPE Disputes*, 99 CORNELL L. REV. 387, 400 (2014) (average legal cost to defend a patent suit ranges from "$420,000 for small and medium-sized companies to $1.52 million for large companies.").

[99] *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 555-59 (4th ed. 1992) (as stakes and uncertainty increase, the probability of settlement decreases and litigation costs increase). *See also* Christopher M. Holman, *Unpredictability in Patent Law and its Effect on Pharmaceutical Innovation*, 76 MO. L. REV. 645 (2011).

[100] *See, e.g.*, Andrew A. Schwartz, *The Corporate Preference for Trade Secret*, 74 OHIO ST. L.J. 623 (2013); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311 (2008).

[101] *See* Patents by Organization, U.S. Patent & Trademark Office, available at http://www.uspto.gov/web/offices/ac/ido/oeip/taf/topo_14.htm. *See also* Annette I. Kahler, *Examining Exclusion in Woman-Inventor Patenting: Historical, Economic and Social Perspectives*, 19 AM. U. J. GENDER, SOC. POL'Y & L. 773, 785-89 (2011).

[102] National Science Foundation, *Women, Minorities, and Persons with Disabilities in Science and Engineering* (2015) (women receive bachelor's degrees in certain science fields at far lower rates than men, including computer sciences (18.2%), engineering (19.2%), physics (19.1%), and mathematics and statistics (43.1%)).

[103] U.S. Department of Labor, Bureau of Labor Statistics, *Women in the Labor Force: A Databook* (2014) (39% of chemists and material scientists are women; 27.9% of environmental scientists and geoscientists are women; 15.6% of chemical engineers are women; 12.1% of civil engineers are women; 8.3% of electrical and electronics engineers are women; 17.2% of industrial engineers are women; and 7.2% of mechanical engineers are women).

[104] For a discussion of using evidence of patents as a measure of economic innovation, please see, e.g., JACOB SCHMOOKLER, INVENTION AND ECONOMIC GROWTH (1966); Zvi Griliches, Ariel Pakes & Bronwyn H Hall, *The Value of Patents as Indicators of Inventive Activity,* NBER Working Paper No. 2083 (1986); Bjørn L Basberg, *Patents and the Measurement of Technological Change: A Survey of*

million utility patents granted by the PTO between 1976 and 2013 found that "[w]omen contributed less than 8% of all inventorships for the entire period," maxing out at 10.8% in 2013, an increase from 2.7% in 1976. Men dominate patenting in almost every country, with 42 countries listing no female inventors whatsoever.[105] Among academic life science patentees, women patent at about 40% the rate of men.[106] And gender inequality in the patent world does not stop there: Historically, women were not only discouraged from claiming credit for their inventions; their innovations were actively co-opted by husbands, fathers, brothers, and other men around them.[107] As Dan Burk has suggested, the continued underrepresentation of women among patentees and patent examiners may suggest that "the system retains some residue" of more overt historical discrimination.[108] Any part of that system that privileges corporate inventors to the exclusion of a more diverse innovator pool contributes to that residual imbalance.

Underlying these practical problems is a broader doctrinal failure. At its heart, the public use bar is about disclosure, a transfer of information from one person, or one party, to another. As such, it is a distinctly social phenomenon that is fact-specific and highly contextual.[109] And yet the principles of privacy as control, which, as discussed *supra*,[110] locate analysis within the disclosing party rather than in the social context of disclosure, dominate the doctrine. Judges tend to focus on the inventor's volitional acts and secondarily, if at

---

the Literature, 16 RESEARCH POLICY 131 (1987); Zvi Griliches, *Patent Statistics Indicators as Economic Indicators: A Survey*, 28 J. ECON. LIT. 1661 (1990)

[105] Cassidy R. Sugimoto, Chaoqun Ni, Jevin D. West, and Vincent Larivière, *The Academic Advantage: Gender Disparities in Patenting*, PLOS.ORG, available at http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0128000#pone.0128000.ref009. *See also* Office of Elec. Info. Prod., U.S. Patent & Trademark Office, U.S. Patenting by Women: 1977-2002 (2003) (on file with author) [hereinafter U.S. Patenting by Women]. *See also* U.S. Patenting by Women, 1977 to 1996, in U.S. Pat. & Trademark Off., U.S. Dep't of Commerce, Buttons to Biotech, 1996 Update Report with Supplemental Data Through 1998 (1999), available at http:// www.uspto.gov/web/offices/ac/ido/oeip/taf/wom_98.pdf.

[106] Waverly W. Ding, Fiona Murray, and Toby E. Stuart, *Gender Differences in Patenting in the Academic Life Sciences*, 313 SCIENCE 665, 666 (2006).

[107] *See* Kahler, *supra* note 101. *See also, e.g.*, JUDY WAJCMAN, FEMINISM CONFRONTS TECHNOLOGY 16 (1991); Zorina Khan, *Married Women's Property Laws and Female Commercial Activity: Evidence from US Patent Records, 1790-1895*, 56 J. ECON. HIST. 356 (1996); Deborah Merritt, *Hypatia in the Patent Office: Women Inventors and the Law, 1865-1900*, 35 AM. J. LEGAL HIST. 235 (1991); Carroll Pursell, *Women Inventors in America*, 22 TECH. & CULT. 545, 546 (1981).

[108] Dan L. Burk, *Do Patents Have Gender?*, 19 AM. U. J. GENDER SOC. POL'Y & L. 881, 887 (2011).

[109] Waldman, *supra* note 6, at 335 ("privacy is a social phenomenon not merely because other people exist, but because privacy is about the social circumstances in which information flows from one party to another.").

[110] *See supra* notes 27-47 and accompanying text.

all, consider the context in which those acts occurred. Only rarely are social norms respected like they are in *Bernhardt*, and when they are, corporate inventors are usually the beneficiaries.

In cases like *Bernhardt*, *Dey*, and *American Seating*, the Federal Circuit acknowledged that the relationship between the inventor and those to whom she discloses her invention should matter because certain relationships could gives rise to an expectation of confidentiality. In *Bernhardt*, the court accepted that participants in the pre-market furniture show could have a custom of confidentiality based on their status as industry partners.[111] In *Dey*, the court recognized that patients in clinical trials typically do not sign confidentiality agreements, so, given that custom, none should be required in this case.[112] And in *American Seating*, the Federal Circuit affirmed that even without confidentiality agreements, the disclosure to a business partner who helped build the invention and the internal demonstration to the inventor's employees were both done in contexts of implied confidentiality.[113]

But those relationships are ignored in Cluster B (solo entrepreneur) cases. If anything, the relationships between the parties in *Beachcombers* (friends and colleagues), *Lough* (friends and colleagues), and *MIT* (friends) were closer and less in need of formal agreements than the relationships in *Bernhardt* (participants in the same business), *Dey* (clinical trial designers and patients), and *American Seating* (business partners and employees) and yet all three of the former lost their public use cases. Elsewhere, district courts, the Federal Circuit, and the Supreme Court have gone out of their way to disclaim any relevance of the relationship between the parties for determining confidentiality or control.[114] However, disclosures of all kinds happen in context, one that, I argue, is characterized by social network trust.

II. Trust and Social Network Confidentiality

To address these doctrinal and practical deficiencies, this Article proposes a reorientation of public use law around three principles: that it should apply equally and evenly to corporate and entrepreneurial inventors alike; retain fidelity to the goals of patent law, in general, and the public use bar, in particular; and reflect the

---

[111] Bernhardt, 386 F.3d at 1381.

[112] Dey, 715 F.3d 1357-58.

[113] American Seating, 514 F.3d at 1268; American Seating Co. v. USSC Group, Inc., No. 1:01-CV-578, 2005 WL 1224603, *4-*5 (W. D. Mich. May 23, 2005)).

[114] *See, e.g.*, MIT, 584 F. Supp. 2d at 313 (citing Egbert v. Lippmann, 104 U.S. 333, 335-38 (1881) ("The Supreme Court has held, however, that even the use of an invention by the inventor's wife or romantic interest could be an invalidating public use. Therefore, the identity of the drivers does not, by itself, prevent the field trials from being a 'public use.'") (internal citations omitted)).

social context of disclosure.[115] Though hardly controversial, these elements have been missing from the doctrine and its application: the law adheres to the individual-focused conception of privacy as control, privileges corporate inventors over solo entrepreneurs, and perversely discourages patenting among some innovators. And yet, these principles make intuitive sense.

At its core, the public use bar is a limitation on disclosure. Social scientists have shown that there are several factors at play in the disclosure of information to small groups: the structure of the network in which the information is disclosed, the nature of the information itself, and the relationship between the disclosing party and the members of her network.[116] Together, studies suggest, these factors help determine the circumstances in which information disclosed to a small group will escape to a larger one. We can apply these factors to achieve our goal of fair public use jurisprudence. I argue that different networks can develop powerful norms of confidentiality and discretion—commonly understood as trust—on which individuals (and inventors) should be able to rely. When disclosures happen in these contexts of trust, they are not public and should be protected as such.

In this section, I summarize the basic principles of social network theory and what I have called, privacy as trust; capture the lessons of that literature for disclosure and public use contexts; translate those lessons into a flexible, network-based, and administrable tool for public use cases; and show how elements of this proposal will not only advance the policy goals of patent law, but are also readily reflected across intellectual property regimes.

A. A Theory of Trust and Information Flow

Social network theory gets us part of the way to our goal. It helps explain how and why certain information may flow through a network and into another, wider network, and why other types of disclosure may not. But it does not explain why we share in the first place. This is the role of interpersonal trust. Together, trust and social network theory provide a step-by-step model that assesses the

---

[115] *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010) [hereinafter NISSENBAUM, PRIVACY IN CONTEXT]; Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) (arguing that contextual integrity is the appropriate benchmark of privacy); Edward Tverdek, *What Makes Information "Public"?*, 22 PUB. AFFAIRS Q. 62 (2008); Waldman, *supra* note 6.

[116] The discussion that follows is based on extensive social science research from the author's doctoral studies and reflects the contributions of legal scholars like Lior Strahilevitz, who's article, *A Social Networks Theory of Privacy*, bridged social network and privacy scholarship, Strahilevitz, *supra* note 42, and Duncan Watts's groundbreaking work on so-called "small world networks." DUNCAN J. WATTS, SIX DEGREES: THE SCIENCE OF A CONNECTED AGE (2003).

reasonableness of disclosures and the likelihood of subsequent publicity. Therefore, they are perfect tools for public use law reform.

1. Social Networks and Information Diffusion

Social network theory is the cross-disciplinary study of how the structure of networks affects behavior.[117] A network is just a set of objects[118]—people, cells, power plants—with connections among them—social encounters, synapses, grids. They are all around us: A family is a (social) network, as is the (neural) network in a brain and the (distribution) network of trash pick-up routes in New York City. To see one visualization of diffusion through a network,[119] dab the nib of a marker into the middle of a piece of construction paper and you will see, in real time, the diffusion of ink from one origin point, or node, through the lattice-like network of fibers that make up the paper. Facebook is the paradigmatic modern social network: its overarching network has nearly 1.5 billion nodes (members),[120] but it also has billions of subnetworks, where nodes overlap, interact, and share information. It is a network's ability to invite, disseminate, and retain information that concerns us.

As Lior Strahilevitz has shown, the theory of information flow within and among networks can begin the discussion of when information disclosed to a small group is still private.[121] It helps establish two important conclusions: that both the structure of a network and the nature of information disclosed into it affect the flow of information through and beyond it.

Although networks are evolving ecosystems[122]—people constantly drop in and out—human social networks tend to be close knit and highly "clustered,"[123] with "strong ties" linking us to our friends.[124] Family members are good examples of individuals with

---

[117] WATTS, *supra* note 116, at 28.

[118] *Id.* at 27.

[119] Network structure is diverse. A simple search of "network visualization" in Google Images shows the wide range of visual representations of networks. *See* https://www.google.com/search?q=network+visualization&espv=2&biw=1680&bih=881&source=lnms&tbm=isch&sa=X&ved=0CAYQ_AUoAWoVChMIyLeWnPrYxgIVTFU-Ch0clg3n.

[120] Facebook Stats, at http://newsroom.fb.com/company-info/.

[121] Strahilevitz, *supra* note 42, at 946-973. For Professor Strahilevitz, the conversation starts at ends with social network theory. *But see* Waldman, *supra* note 6, at 335-36, 366-70.

[122] WATTS, *supra* note 116, at 28.

[123] *Id.* at 40; Strahilevitz, *supra* note 42, at 951 (*citing* Ronald S. Burt, *Bridge Decay*, 24 SOC. NETWORKS 333, 333-34 (2002) and Karen Klein Ikkink and Theo van Tilburg, *Broken Ties: Reciprocity and Other Factors Affecting the Termination of Older Adults' Relationships*, 21 SOC. NETWORKS 131, 142-45 (1999)).

[124] Mark Granovetter, *The Strength of Weak Ties*, 78 AM. J. SOC. 1360, 1361 (1973).

strong ties: everyone knows everyone else and each member engages in repeated social interactions with each other. They spend a lot of time with each other, have deep emotional connections, and reciprocate the connection with each other.[125] Members of other tightly clustered networks—support groups, recreational sports teams, individuals with the same political beliefs—share with each other. Social network theory does not tell us precisely *why* these persons feel comfortable sharing personal information with each other, but it does explain one form of information diffusion. The stronger the tie between two individuals, the more likely their friends overlap, and the more likely information will stay within those close-knit overlapping networks. If networks only had strong ties, we would see many groups of friends that recycle information among themselves.[126] Based on this research, we can conclude that disclosures among closely-knit strong ties will rarely diffuse to the wider public.

Information is also spread between different clusters through what Mark Granovetter has called "weak ties."[127] Some weak ties are "supernodes," or society's socialites:[128] They have close friends in different groups and make connections among them. One example might be an in-law. My sister is part of my close knit family network; her husband is part of his. If he is indeed close to his family and a social person, he could perform the function of a network bridge supernode, making connections between disparate people like me—a gay law professor who lives in New York City and enjoys hiking and watching ballet—and his younger brother—a married heterosexual who dislikes lawyers and used to wrestle in high school.

More often than not, though, people are linked by the acquaintances they share—two strangers on a train marveling that they have the same mutual friend.[129] These weak tie bridges, Professor Granovetter has shown, are the driving force behind information dissemination from one close-knit group to another.[130] These weak ties are acquaintances we don't know well, but with whom interactions are essential if we want to bring outside information into a close-knit group full of strong ties.[131] Consider

---

[125] *Id.*

[126] *Id.* at 1366 ("If one tells a rumor to all his close friends, and they do likewise, many will hear the rumor a second and third time, since those linked by strong ties tend to share friends. … [B]ridges will not be crossed.")

[127] *Id.* ("whatever is to be diffused can reach a large number of people, and traverse greater social distance (i.e., path length), when passed through weak ties rather than strong.").

[128] Strahilevitz, *supra* note 42, at 951.

[129] WATTS, *supra* note 116, at 41. Duncan Watts's project, the "small world problem," is so named after the reaction when two strangers realize they have a friend in common. They say, "what a small world!"

[130] Granovetter, *supra* note 124, at 1366.

[131] WATTS, *supra* note 116, at 49 (*citing* Granovetter, *supra* note 124).

another example: Jennifer is a doctor, a soccer mom, and a hiker; she is friends with her colleagues, casually acquainted with her child's teammates' moms and dads, and is very close with her hiking buddies, with whom she goes on an annual trip to Machu Pichu. An occasionally random conversation at work or at a soccer game about hiking may introduce a love for the outdoors to soccer dad who has lived all his life in an urban environment. Professor Granovetter has shown that these types of weak ties are essential to, among other things, getting jobs:[132] weak ties bring in contacts and information you would not otherwise have received.[133] When there are no weak ties between individuals otherwise connected by only a few steps, or when those ties are inactive, those even nearby nodes are highly unlikely to ever encounter each other or the information they disseminate. They have what Ronald Burt has called a "structural hole" between them.[134] As the active bridges between close-knit groups, then, weak ties are essential for information diffusion.

But the structure of the network—clustering, distance between clusters, and types of connections, as well as any exogenous limitations to the network—is not the only important element. The nature of the information also matters. Weak ties are not adept at transmitting all types of information. Job opening or rumors are easy to pass along: they are simple pieces of information that do not degrade along the line and are, therefore, amenable to transmission during short chance encounters with acquaintances.[135] But studies have shown that they are ill equipped to transfer complex information or aggregate pieces of information into a richer picture.[136] In other words, weak ties cannot put two and two together to make four; conversations with acquaintances rarely involve in-depth analysis.

Professor Strahilevitz illustrated these points using the popular parlor game, "Six Degrees of Kevin Bacon."[137] Duncan Watts used stories from his own life.[138] Facebook is another helpful,

---

[132] Granovetter, *supra* note 124, at 1371-73.

[133] Weak ties are, therefore, essential to overcoming the problem Cass Sunstein described in Republic.com 2.0, where he argued that online social networks contribute to greater political polarization in society because network algorithms reinforce individuals' choices to seek out information with which they already agree. *See* CASS R. SUNSTEIN, REPUBLIC.COM 2.0 (2009).

[134] Strahilevitz, *supra* note 42, at 952 (*quoting* RONALD S. BURT, STRUCTURAL HOLES: THE SOCIAL STRUCTURE OF COMPETITION 18 (1992)).

[135] Gabriel Weimann, *The Strength of Weak Conversational Ties in the Flow of Information and Influence*, 5 Soc. Networks 245, 254-55 (1983); Morton T. Hansen, *The Search Transfer Problem: The Role of Weak Ties in Sharing Knowledge Across Organizational Subuits*, 44 Admin. Sci. Q. 82, 105 (1999) (*quoted in* Strahilevitz, *supra* note 42, at 957).

[136] Strahilevitz, *supra* note 42, at 957-58.

[137] *Id.* at 949-52.

[138] WATTS, *supra* note 116, *et seq.*

accessible model. Facebook is an evolving ecosystem, where new people are always joining and dropping out, changing our own social networks. The average Facebook user has 338 friends,[139] but "follows" far fewer, with fewer still showing up on her news feeds.[140] This sub-network of friends tends to be close-knit, constituted by many overlapping strong ties. But Facebook's algorithm, while privileging close friends, allows posts from acquaintances in our networks to appear on our feeds, as well. These weak ties bring in additional information from outside our closest-knit groups. The type of information also matters: studies show that status updates, shared links, and photos reach more members of your network than friendships and wall posts.[141]

2. Trust and Sharing

But social network theory does not explain why we share information with others—strong or weak ties, intimate friends or strangers—in the first place. As an information flow model, it skips the first step: social network models help explain how the ink spreads through the construction paper, not why we placed the marker nib on the paper in the first place. But this is essential for developing an administrable model for adjudicating public use cases: the initial disclosure to others has to be reasonable, not reckless, and one that society, and by extension, the law is willing to protect.[142] This is the role of trust.[143]

Trust is the favorable "expectation regarding … the actions and intentions"[144] of particular "people or groups of people, whether known" or unknown, whether "in-group" or out-group.[145] Trust is

---

[139] Aaron Smith, *6 New Facts about Facebook*, Pew Research Center, at http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/.

[140] Sharon Gaudin, *Social Network Changes Algorithm to Make 3 Changes to Users' News Feed*, COMPUTER WORLD, Apr. 22, 2015, at http://www.computerworld.com/article/2913017/social-media/facebook-gives-priority-to-friends-in-news-feed-change.html.

[141] Josh Constine, *Your Average Facebook Post Only Reaches 12% Of Your Friends*, TECHCRUNCH, Feb. 29, 2012, at http://techcrunch.com/2012/02/29/facebook-post-reach-16-friends/.

[142] This is also true of personal disclosures in the privacy context. Individuals retain privacy rights where they have a legitimate expectation of privacy that society is willing to recognize as reasonable. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[143] Trust has been experiencing a revival of late. In addition to my own work on the subject, *see* Waldman, *supra* note 6, Neil Richards and Woodrow Hartzog argue that privacy should be conceptualized as a means of building trust. *See* Neil Richards and Woodrow Hartzog, *A Theory of Privacy and Trust* (manuscript on file with author).

[144] *See* Guido Möllering, *The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension*, 35 SOCIOLOGY 403 (2001).

[145] Ken Newton & Sonja Zmerli, *Three Forms of Trust and Their Association*, 3 EUR. POL. SCI. REV. 169, 171 (2011).

bound up with our expectations of others' behavior, and it begins where precise knowledge of others' behavior ends. For example, Alice and Brady are friends, and Brady has always watched Alice's dog when she's away on business. Her knowledge ends there. But Alice still trusts that when she asks Brady to watch her dog next time, he will do so. Alice trusts that her friends will continue to act as friends. We trust that a moving car, though moving slowly, will stop at a stop sign. We trust our therapists to keep our secrets. We trust that the 5:43 AM train to Penn Station will depart at (approximately) 5:43 AM.

This kind of trust is what sociologists call particularized social trust: it is interpersonal, directed at specific other people or groups, and forms the basis of person-to-person interaction.[146] It allows us to take risks,[147] cooperate with others,[148] make decisions despite complexity,[149] and create order in chaos,[150] among so many other everyday functions. Trust's positive effects on society are based on its role as a social lubricant: it is essential to all social interaction and is at the heart of why we decide to share personal or sensitive information with others.[151]

Gene Shelley's study of sharing HIV-status with others illustrates the role of trust in disclosure. HIV-status is, for many, private, but not secret: many of the same people that choose to hide their status from acquaintances, friends, and even family for fear of ostracism, stigmatization, homophobia, or worse,[152] are willing to share it with relative strangers who are also living with HIV.[153] Several participants in Shelley's ethnography explained why: "I would

---

[146] *Id.* at 170-72.

[147] *See* JAMES S. COLEMAN, FOUNDATIONS OF SOCIAL THEORY 91 (1990) (people take risks that are "depend[ant] on the performance of another actor" because they trust the other actor).

[148] *See* Diego Gambetta, *Forward* to TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS ix, ix (Diego Gambetta ed., 1988) ("cooperation is predicated [on] trust").

[149] *See* NIKLAS LUHMANN, TRUST AND POWER 4 (1979).

[150] *See generally* BARBARA A. MISZTAL, TRUST IN MODERN SOCIETIES: THE SEARCH FOR THE BASES OF SOCIAL ORDER (1996).

[151] *See* Waldman, *supra* note 6. *See also* Ari Ezra Waldman, Privacy as Trust: Sharing Personal Information in a Networked World (2015) (Ph.D. Dissertation) (on file with the Columbia University Library); Ari Ezra Waldman, *Data Report: Trust as a Factor in User Motivations to Share Personal Information on Facebook*, DATA PRIVACY PROJECT AT NEW YORK LAW SCHOOL (forthcoming 2015) (presenting quantitative data showing that trust is a key, statistically significant factor in individuals' decision to share personal information on Facebook).

[152] *See, e.g.*, Laurel Sprague, *Legal Vulnerabilities Related to HIV*, The Sero Project, at http://seroproject.com/wp-content/uploads/2013/07/Young-people-of-color-and-criminalization_Sero-results-2013.pdf.

[153] Gene A. Shelley, et al., *Who Knows Your HIV Status? What HIV+ Patients and Their Network Members Know About Each Other*, 17 SOC. NETWORKS 189, 204 (1995).

tell my support group. Everyone there is HIV-positive and I'm comfortable there."[154] Another stated: "The only two people, aside from members of my support group and doctors, who know are my former lover (who gave her the HIV) and my son's father."[155] Yet another makes the point even clearer: "I told my brother and he said he was (HIV+)."[156]

My own fieldwork suggests that similar principles hold outside the arguably unique support group context. As trust in Facebook increases, members of the social network are willing to post more sensitive information about themselves. Facebook members tend to accept friend requests from strangers when they have similar important identities and when their close friends overlap. Trust—expectations of how Facebook and its members will behave—was the only statistically significant indicator of user behavior.[157]

Neither the structure of the participants' networks nor the nature of the information explains why individuals share private information in the first place. It cannot be the mere fact that a support group is close knit; so is a family, and many respondents adamantly refuse to disclose their status to family members. Individuals on Facebook share information with different subnetworks of friends, as well, many of which look like the close-knit networks discussed above. The explanation for why we share, therefore, has to account for differences among networks. A better explanation is a form of network-specific trust: with respect to preventing the further spread of a person's HIV-status, individuals living with HIV can better predict the future behavior of others also living with HIV (even if they know very little else about them) than others with whom they may be close for different reasons. This unstated implication of Shelley's research suggests that powerful norms of confidentiality and behavior that limit information flow can develop within different social networks depending on structure, the nature of the information, and indicia of trust among members.

The trust at the core of those norms is well known to sociologists. The confident ability to predict others' future behavior develops in several ways. Among people that know each other, trust develops through iterative exchange and, assuming rationality, predictability increases as experience increases.[158] This explains

---

[154] *Id.*

[155] *Id.* (parenthetical in original).

[156] *Id.* at 205.

[157] *See* Waldman, *Data Report*, *supra* note 151.

[158] *See, e.g.*, PETER M. BLAU, EXCHANGE AND POWER IN SOCIAL LIFE 98–99 (1964); John K. Rempel et al., *Trust in Close Relationships*, 49 J. PERSONALITY & SOC. PYCHOL. 95, 96 (1985). *See also* Patricia M. Doney et al., *Understanding the Influence of National Culture on the Development of Trust*, 23 ACAD. MGMT. REV. 601, 605 (1998) ("[T]he greater the variety of shared experiences, the greater the generated

Alice's interactions with Brady. Among acquaintances and strangers, trust develops because individuals share important identities or share trustworthy friends and transfer the trust they have in others they know well.[159] Persons living with HIV will share their status with others living with HIV. Members of the LGBT community are more likely to accept a Facebook friend request from a stranger who is also LGBT.[160] And across all populations, Facebook users are willing to include strangers in their networks and, thus, share information with them, if they share the same close friends.[161] This is what drives our decisions to share personal information in a host of different social networks that may contain distant nodes: our expectations that member behavior will accord with long standing norms give us the confidence to share. That conclusion is network-specific and information-dependent, meaning that a trusting context can vary from network to network and from one piece of information to another. An HIV support group might represent a trusting context when it comes to sharing information about HIV and sex, information that could engender judgment elsewhere. But, for some, it may not be the most appropriate place to admit you work for a conservative member of Congress.

3. Takeaways

If we combine the lessons of privacy as trust with social network theory, one overarching conclusion emerges: Information disclosed in networks characterized by trust is not truly public because it is unlikely to diffuse from one network to another. Relying upon expectations of network members' future behavior based on either previous interactions or a legitimate process of transference, individuals share sensitive information with their network. If it is a network of almost exclusively strong ties, as many informal social networks are, the information is likely to be recycled rather than escape. The presence of weak ties increases the likelihood of information diffusion outside the network. And what constitutes a strong or a weak tie may vary with the information at issue. As will the ease of diffusion: complicated information generally does not travel through weak ties, but what is simple to one audience may be complex to another. The greater the audience's applicable skill level relative to the information, the more likely it falls on the simpler end of the information spectrum.

---

knowledge base and the more a target's behavior becomes predictable.") (citation omitted); David Good, *Individuals, Interpersonal Relations, and Trust*, in TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 31, 32 (Diego Gambetta ed., 1988); Michael W. Macy & John Skvoretz, *The Evolution of Trust and Cooperation Between Strangers: A Computational Model*, 63 AM. SOC. REV. 638, 648, 655–56 (1998).

[159] Waldman, *Privacy as Trust*, *supra* note 6, at 348-49.

[160] Waldman, *Data Report*, *supra* note 151.

[161] *Id.*

We can apply these lessons to developing a model for analyzing public use cases. First, the test for public use must be a totality of the circumstances test. This kind of flexible standard is the only way to assess a social context on a case-by-case basis. Second, the test should focus on (1) the information disclosed, (2) the network into which inventions are disclosed, looking for weak ties likely to spread the information and strong ties that do not, and assessing relative complexity of the information, and (3) the relationship between the parties, looking for indicia of trust based on experience, identity, overlapping networks, transference, and other indicators. Third, some of the questions fact-finders should ask include, but may not be limited to, the following: Did the relationship between the inventor and her audience show any evidence of implied confidentiality? Was the demonstration or use of the invention done in such a way so as to reveal to the audience how it worked? Was the invention complex, especially relative to the skill level of the audience? Did the audience contain acquaintances, strangers, or other individuals not bound by any of the traditional models of interpersonal trust? And, did the audience contain "supernodes" that could bridge networks?

These questions can help fact finders establish the expectations of all parties involved in an alleged public use. Notably, these questions do not prevent a court from considering other factors, including the presence of confidentiality agreements and evidence of commercial motive for the use. The new standard merely ensures that neither formal agreements nor commercial intent is elevated to determinative status and that the locus of analysis shifts from the individual to the social context of disclosure.

B. Advantages to the Approach: Social Networks and Intellectual Property

Applying privacy as trust to public use questions has all the advantages missing from the current privacy as control approach: it is egalitarian, flexible, practical, and retains fidelity to the policy objectives of patent law. Nor is it a radical proposal: the respect for social network theory embedded in privacy as trust already cuts across all intellectual property regimes. This Article's flexible, network-oriented approach to public use will, therefore, fit neatly within our intellectual property legal traditions.

Privacy as trust will end the current system's uneven and unfair application. As discussed above, it privileges corporate inventors over solo entrepreneurs[162] in two ways: respecting industry norms of confidentiality while ignoring the more informal social norms of friends,[163] and elevating the importance of formal

[162] *See supra* Part I.B.
[163] *See supra* Part I.B.2.

confidentiality agreements to near determinative status.[164] The first tendency directly benefits the already entrenched interests of corporate patentees; the second tendency indirectly enhances their position, as well, because only wealthy inventors have the leverage to insist on nondisclosure agreements and the money to pay lawyers to write them. These discriminatory applications are an outgrowth of employing a privacy as control standard: it lends itself to bright line rules regarding disclosure and ignores the social context in which an inventor decides to demonstrate her invention.[165]

Privacy as trust gives judges the tools to reverse these tendencies. It does not discriminate between social networks; indeed, the proposal is built around the notion that different social networks can create equally powerful norms of confidentiality and low likelihoods of information diffusion beyond the network. And by shifting the public use analysis from the inventor's actions to the social context of disclosure, it ensures that myriad factors beyond signed confidentiality agreements will be in play. In turn, inventors and entrepreneurs traditionally underrepresented in the corporate world will be given a fair shot.

It also remains true to the goals of patent law, in general, and the public use bar, in particular. As expressed by the Federal Circuit outlined in *Tone Brothers v. Sysco*,[166] those goals are

> (1) discouraging the removal, from the public domain, of inventions that the public reasonably has come to believe are freely available; (2) favoring the prompt and widespread disclosure of inventions; (3) allowing the inventor a reasonable amount of time following sales activity to determine the potential economic value of a patent; and (4) prohibiting the inventor from commercially exploiting the invention for a period greater than the statutorily prescribed time.[167]

Inventions disclosed to close friends or colleagues whom we trust cannot truly be said to be "freely available" in any sense. Prompt disclosure and patenting is still incentivized by the America Invents Act's first-to-file rule. And there is less likely to be evidence of commercial exploitation or sales activity in situations of disclosures to social friends and other trusted social networks. Indeed, looking to relationships of trust may advance the goals of the patent system: it would encourage more experimentation among corporate inventors and lone entrepreneurs alike. As the Supreme Court said in 1877, it does not frustrate the public interest when delays in patenting are

---

[164] *See supra* Part I.B.1.
[165] *See supra* Part I.C.
[166] 28 F.3d 1192 (Fed. Cir. 1994).
[167] *Id.* at 1198.

"occasioned by a bona fide effort to bring [the] invention to perfection, or to ascertain whether it will answer the purpose intended."[168] The patent monopoly is, after all, only temporary, "and it is the interest of the public, as well as [the inventor's], that the invention should be perfect and properly tested, before a patent is granted for it."[169] A respect for relationships of trust among inventors and their friends and colleagues would not only help realize this goal, but it would also challenge the results in cases like *Beachcombers*, *Lough*, and *MIT*.

Beyond these policy benefits, the network-oriented approach of privacy as trust occupies an underappreciated yet salient position across intellectual property law, making it even more reasonable to apply it to public use cases. As I have discussed in detail elsewhere,[170] social network theory permeates all branches of intellectual property. Copyright's originality threshold,[171] for example, which requires a bare modicum of creativity to obtain a copyright,[172] is defined relative to the industry norms in which the creator belongs. In *Feist Publications v. Rural Telephone Services*,[173] for example, the seminal Supreme Court case on copyright originality, a run-of-the-mill phonebook was not copyrightable because it was designed, arranged, and presented in an ordinary manner. But "ordinary" was defined relative to the closed network of other phone books. Rural's local phone book was "typical,"[174] unlike Feist's, which covered a wider area and included additional data.[175] In the end, the reason why Rural's local phonebook was not copyrightable was because it was just like every other *phonebook*: "Rural's white pages are entirely *typical*. … The end product is a garden-variety white pages directory, devoid of even the slightest trace of creativity."[176] Typicality is, by definition, entirely contextual and based on the customs and norms of a particular field, i.e., something is typical compared to something else.

---

[168] *See* City of Elizabeth v. Am. Nicholson Pavement Co., 97 U.S. 126, 137 (1877).

[169] *Id.*

[170] Ari Ezra Waldman, *Social Networks and Intellectual Property: Revisiting Professor Zittrain's IP and Privacy "Problem"* (forthcoming) (manuscript on file with author).

[171] 17 U.S.C. § 102 ("Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression").

[172] Feist Publications, Inc. v. Rural Tel. Servs. Co., Inc., 499 U.S. 340, 358 (1991) ("Originality requires only that the author make the selection or arrangement independently (i.e., without copying that selection or arrangement from another work), and that it display some minimal level of creativity.).

[173] 499 U.S. 340 (1991).

[174] *Id.* at 342 ("Rural publishes a typical telephone directory").

[175] *Id.* at 342-43 ("Unlike a typical directory, which covers only a particular calling area, Feist's area-wide directories cover a much larger geographical range.").

[176] *Id.* at 362.

It is typical for phone books to be alphabetical. It is not typical for, say, epic poems to be alphabetical listings of words.

Differences among social networks are also embedded in trademark law, which is principally concerned with protecting brands and preventing consumer confusion.[177] Among the several factors courts use to assess consumer confusion under the Lanham Act,[178] three take a network-specific approach: The more related the products and the more overlap in marketing channels, the greater the likelihood of a confusion finding, presuming that products that target different networks are less likely to be the subject of confusion. Courts also assess the degree of care likely to be exercised by purchasers, implicitly recognizing that different consumers behave differently. Consumer confusion, therefore, is an information flow problem, but one that reflects how information diffuses from one network to another.[179]

And, like copyright's originality threshold, patent law's substantive requirements of patentability take a network-oriented approach. Inventions that are obvious to someone "having ordinary

---

[177] Scholars generally agree that the goals of trademark law are to prevent consumer confusion, protect brand goodwill, and promote fair competition. They sometimes disagree on which goal merits the greatest emphasis. *See, e.g.*, Robert G. Bone, *Hunting Goodwill: A History of the Concept of Goodwill in Trademark Law*, 86 B.U. L. REV. 547, 549, 555-56 (2006) ("The major focus of trademark law is protecting the source identification and information transmission function of marks."); Jennifer E. Rothman, *Initial Interest Confusion: Standing at the Crossroads of Trademark Law*, 27 CARDOZO L. REV. 105, 127 (2006). *See also* Qualitex Co. v. Jacobsen Products Co., 514 U.S. 159, 163-64 (1995) ("In principle, trademark law, by preventing others from copying a source-identifying mark, 'reduce[s] the customer's costs of shopping and making purchasing decisions,' for it quickly and easily assures a potential customer that this item—the item with this mark—is made by the same producer as other similarly marked items that he or she liked (or disliked) in the past. At the same time, the law helps assure a producer that it (and not an imitating competitor) will reap the financial, reputation-related rewards associated with a desirable product.").

[178] There are eight such factors: "similarity of the conflicting designations; relatedness or proximity of the two companies' products or services; strength of [the senior] mark; marketing channels used; degree of care likely to be exercised by purchasers in selecting goods; [alleged infringer's] intent in selecting its mark; evidence of actual confusion; and likelihood of expansion in product lines." *See, e.g.*, Brookfield Comm's, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1054 (9th Cir. 1999); AMF, Inc. v. Sleekcraft Boats, 599 F.2d 341, 348-49 (9th Cir. 1979). But, as the Ninth Circuit stated in *Brookfield*, some factors, particularly the first three, are "more important than others." Brookfield, 174 F.3d at 1054.

[179] Jonathan Zittrain has argued that the "problem" of privacy is the same as the "problem" of intellectual property: dissemination of information and the loss of personal control. Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201 (2000). I argue that that Professor Zittrain is correct, to a point: the problem is not just information dissemination, but dissemination to a different network. *See* Waldman, *Social Networks*, *supra* note 170, at __.

skill in the art," or PHOSITA,[180] are unpatentable.[181] Patent applications that cannot teach the PHOSITA how to make or use the invention are also invalid.[182] And when courts construe patent claims, the words in the patent that define and delimit the world of inventions captured by the patent, they do so in light of what the person of ordinary skill would understand.[183] Therefore, what would be obvious, enabling, and understandable to a mechanical engineer might be different from what is obvious, enabling, and understandable to a computer scientists, biologist, or chemist. And their level of understanding is certainly different from that of the public at large.

Trade secret law goes even further than recognizing that social networks exist. In fact, without ever using the language of social network theory and trust, trade secrecy employs the network-oriented, trust-based model described above in three ways. First, a trade secret is defined relative to a given network. Although the rule is that information "generally known or readily ascertainable to the public" cannot constitute a trade secret, the "public," in this case, refers to a given industry.[184] The rule makes sense as a matter of economics and competition, but it also reflects the social science of information diffusion. An oil company executive might come across the proprietary recipe of a donut company,[185] but unless there are weak tie bridges ready to disseminate the recipe beyond the oil industry and, somehow, to the confections business, the information is unlikely to get to those who could use it.[186]

A second lesson of social network theory—that weak tie bridges between networks are ill equipped to disseminate complex or aggregated information[187]—is also reflected in the law of trade secrets. As the Fifth Circuit stated in *Metallurgical Industries v. Fourtek*,[188] a seminal and oft-cited trade secrets case, the aggregation of pieces of information, "each of which, by itself, is in the public domain," can be a trade secret because knowledge and aggregation of

---

[180] *See, e.g.*, John O. Tresansky, *PHOSITA—The Ubiquitous and Enigmatic Person in Patent Law*, 73 J. PAT. & TRADEMARK OFF. SOC'Y 37, 37 (1991).

[181] 35 U.S.C. § 103 (2015). This is the requirement of non-obviousness.

[182] 35 U.S.C. § 112(a) (2015). This is the enablement requirement.

[183] *See, e.g.*, Xerox Corp. v. 3Com Corp., 458 F.3d 1310, 1323-24 (Fed. Cir. 2006).

[184] *See, e.g.*, Research & Dev. Corp. v. Nat'l Chem. Co., 87 F.3d 937, 942 (7th Cir. 1996); Zoecon Indus. v. Am. Stockman Tag Co., 713 F.2d 1174, 1179 (5th Cir. 1983) (a trade secret cannot be known by others *in the same business*) (emphasis added).

[185] The recipe for Krispy Kreme donuts is a famous trade secret.

[186] For a discussion of Mark Granovetter's theory on the "strength of weak ties" and the role they play in information diffusion, see *supra* notes 121-141 and accompanying text.

[187] *See supra* note 136 and accompanying text.

[188] 790 F.2d 1195 (5th Cir. 1986).

those bits of data could provide a competitive advantage.[189] Again, the economic rationale makes sense. But implicit in this aggregation rule is the assumption that industry competitors are not adept at piecing together bits of distant data points or, to use the language of social network theory, that complex and aggregated information does not diffuse through networks easily and is unlikely to be gathered up, analyzed, and put to use through weak ties. Otherwise, the aggregate information could not be considered a secret in any sense.

Third, when it comes to the prior disclosure of confidential business information, a problem similar to pre-patenting use, trade secret law takes a network- and relationship-oriented approach, unconsciously implementing some of the lessons of social network theory and trust. As Sharon Shandeen showed in her cross-disciplinary study of privacy and trade secrecy,[190] trade secret law embraces the doctrine of "relative secrecy."[191] This is the notion that legal protection for trade secrets can be retained even when others know the secret. The test for determining when such protection exists "is contextual and depends on a number of factors, not the least of which is the relationship … between the trade secret owner and the person(s) to whom the information is disclosed."[192] Trade secrecy, then, shifts the analysis to the context of disclosure, finding duties of confidentiality implied by the norms of those contexts. Professor Shandeen gathered and analyzed the case law and found that a diverse arrays of relationships has given rise to implied confidentiality: employer and employee, purchaser and supplier, licensor and licensee, and between partners in joint ventures, among others.[193] Trade secret cases also appreciate the role of norms created by these relationships rather than just the formalities themselves. As one court stated: "To give publicity wantonly and confidentially correspondence meets with the prompt rebuke and merited condemnation of every one not lost to all honorable feeling. It is a

---

[189] *Id.* at 1202. *See also, e.g.*, Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1291 (11th Cir. 2003); Catalyst & Chem. Servs., Inc. v. Global Ground Support, 350 F. Supp. 2d 1, 9 (D. D.C. 2004) ("Defendants have submitted exhibits showing that each parameter individually was within industry knowledge before defendants' alleged disclosure. Plaintiffs, however, do not allege only that each parameter individually is a trade secret; rather, they also argue that all four elements taken together in precise combination constitute a legally protected interest under the Trade Secrets Act. The record does not show that all four parameters were disclosed together, in a specific combination, to the industry.") (internal citations omitted).

[190] Sharon Shandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667 (2006).

[191] *Id.* at 696. Also the topic of Professor Strahilevitz's article, *A Social Networks Theory of Privacy*. *See* Strahilevitz, *supra* note 42.

[192] John C. Stedman, *Trade Secrets*, 23 Ohio St. L. J. 4, 6 (1962) (*quoted in* Shandeen, *supra* note 190, at 697).

[193] Shandeen, *supra* note 190, at 699.

death-blow to the best interests of civilized society itself."[194] Lofty rhetoric aside, trade secret law appreciates norms of trust and confidentiality implied by certain social contexts.

What is missing from trade secrecy's approach to the problem of limited disclosures, and why public use law cannot simply learn the lessons of "relative secrecy" and move on, is a model for solving the public use's discrimination problem. Relative secrecy cases often involve corporate parties and, as Professor Shandeen has shown, the relationships that courts have so far recognized as giving rise to implied duties of confidentiality are business relationships. That confidentiality agreements are not required, in doctrine and in practice, is a step forward. But trade secrecy does not get us any further toward respecting the powerful confidentiality norms of networks of friends, solo entrepreneurs, part-time inventors, and hobbyists. A social network-based doctrine of trust does just that.

III. Reorienting Public Use Law

Armed with the lessons of social networks and privacy as trust, we can return to the public use cases discussed above and summarized in Figure I. Recall that sometimes, not having a confidentiality in place has little to no effect on a public use analysis: those cases tend to involve Cluster A (corporate) inventors, who usually win their public use cases. Other times, confidentiality agreements are essential, leading many Cluster B (solo entrepreneur) inventors to lose their public use cases.[195] Even where Cluster A inventors lose, courts' tendencies to elevate formal secrecy agreements to near determinative status is a boon: only inventors with the power and money of a large corporation have the leverage to put nondisclosure commitments in writing and force their business partners to sign them.[196] And where confidentiality agreements are missing, courts tend to be willing to fill the gap with the customs and norms of industry, but rarely do so with the more informal, yet no less powerful norms common to solo inventors, hobbyists, and part-time innovators.[197] In short, the application of the public use bar is either haphazard, at best, or discriminatory, at worst, with no clear tools in the current doctrine to resolve the problem. The dominant theory of adjudication—what privacy scholars would call privacy as control—lends itself to the harsh, bright line, and uneven application of the law. This raises the question of how to reform public use law to create more certainty, fairness, and justice.

Social network theory and privacy as trust offer a model for adjudicating public use cases. Using a totality of the circumstances

---

[194] Roberts v. McKee, 29 Ga. 161, 163 (1859) (*quoted in* Shandeen, *supra* note 190, at 701).

[195] *See supra* notes 57-72 and accompanying text.

[196] *See supra* notes 73-80 and accompanying text.

[197] *See supra* notes 81-96 and accompanying text.

test that focuses on the audience for a disclosure, the information's complexity relative to that audience, and the relationship between the inventor and the audience, the standard will comport with what we know about how and why individuals share information with others. In this section, I revisit some of the leading public use cases discussed above and show how some would turn out the same, others would end differently, and the fate of others requires more information. Luckily, a network- and trust-oriented approach also lays out clear pathways for the admission of evidence, allowing appellate judges to remand cases with specific instructions for fact-finding. I then respond to possible objections to applying privacy as trust to public use.

A. Looking at the Cases Anew

A case like *Xerox v. 3Com*,[198] a Cluster A case, would come to the same result. The analysis would vary only slightly. In *Xerox*, a company employee invented a method that improved computer handwriting recognition.[199] Concluding that the inventor's submission of a videotape of himself demonstrating the invention to conference organizers as part of an application to present did not invalidate his patent, the court explained that the videotape was not a public *use*: No one, other than the inventor, had actually used anything.[200] That can hardly be the rule in public use cases; cases like *Baxter* and *Eolas Technologies v. Microsoft* both found invalidating public uses after mere demonstration by the inventor.[201] But the court did rely on the norms, customs, and practices of the context of the disclosure. Although the inventor did not include a secrecy agreement along with his submission, the court recognized that conference organizers keep submissions confidential as a matter of "professional courtesy and practice" and that they were under "a professional ethical obligation" to maintain secrecy.[202]

This holding makes sense under a social network and trust model, as well. Given the relationship between the inventor and his audience, norms of trust can be implied: academic conference organizers generally do not reveal the details of their submissions. And even if the submission was sent to the two organizers who shared it with a selection committee, that audience was a close-knit closed network of strong ties. As such, the information was unlikely to jump from one small network to another wider network.

---

[198] 26 F. Supp. 2d 492 (W.D.N.Y. 1998).

[199] *Id.* at 493.

[200] *Id.* at 496.

[201] *See* Baxter Int'l v. Cobe Labs., 88 F.3d 1054, 1056, 1058 (Fed. Cir. 1996) (inventor showed others how the centrifuge worked); Eolas Tech. v. Microsoft, 399 F.3d 1325, 1334 (Fed. Cir. 2005) (demonstration to Sun Microsystems employees).

[202] Xerox, 26 F. Supp. 2d at 496.

Under a social network and trust framework, *Moleculon Research v. CBS*[203] would come to the same result, but for very different reasons. Indeed, the analysis of this case highlights the chasm between the current doctrine and application and shows how a social network approach honors the letter and spirit of the law.

Moleculon seems to stand for the proposition that, as with trade secrets' doctrine of "relative secrecy,"[204] the relationship between the inventor and her audience matters for public use. A close look at the Federal Circuit's reasoning shows that, in fact, the likelihood of confidentiality of close-knit networks was ignored. In *Moleculon*, an organic chemistry graduate student and puzzle enthusiast invented what we would now recognize as a device similar to a Rubik's Cube, but did so long before the famous Rubik's Cube puzzle was developed and marketed.[205] He developed various paper models of the device and showed them to close friends, two roommates, and a colleague in the chemistry department. Once employed at Moleculon, the inventor left a wooden version on his desk, where his employer saw it and took an interest in it. After the inventor demonstrated how it worked, they jointly decided that Moleculon would try to market the device, at which point they sent prototype to Parker Brothers and many other toy manufacturers.[206] No one signed confidentiality agreements. Nor, as far as we know, was there any overt discussion of secrecy. The maker of the Rubik's Cube, which Moleculon alleged infringed the patent on its device, challenged the patent's validity for public use: the inventor's decision to show the device to his friends, roommates, colleagues, and boss, they argued, more than met public use's publicity requirement.

The Federal Circuit disagreed, but in so doing, although it professed to focus on the relationships between the parties involved in the disclosures, it really did no such thing. Rather, the court's analysis looked at the volitional acts of the inventor, in line with the strict limits of privacy as control. The court suggested that "the personal relationships and other surrounding circumstances" gave rise to a "legitimate expectation of privacy and of confidentiality" at all times.[207] But, upon closer examination of the decision, the relationships did not matter. What mattered was that the inventor never physically gave his invention to anyone else and never evinced a commercial motive for his demonstrations. That he at all times retained physical possession was what distinguished this case from *Egbert v. Lippmann*,[208] the 1881 Supreme Court case where the Court said that an inventor made a public use of a corset when he gave it to

[203] 793 F.2d 1261 (Fed. Cir. 1986).
[204] *See supra* notes 190-194 and accompanying text.
[205] Moleculon, 793 F.2d at 1263.
[206] *Id.*
[207] *Id.* at 1266.
[208] 104 U.S. 333 (1881).

his girlfriend to wear under her clothes. It could not have been the relationships between inventor and audience that distinguished *Egbert*; if anything, the implied confidentiality among lovers is stronger than between roommates and colleagues. The only thing that distinguishes *Egbert* is that, in *Egbert*, the inventor physically handed over the corset; in *Moleculon*, he kept it in his hands during demonstration. The Federal Circuit also relied on the inventor's lack of commercial intent in demonstrating his puzzle, reinforcing its focus on whether the inventor gave up control of the device.[209]

Looking at *Moleculon* through the lens of privacy as trust would retain the result (nonpublic use), but employ an analysis far more honest to the law of public use. Close friends and roommates, to whom the puzzle inventor demonstrated his device, represent the kind of close-knit strong ties that recycle information within a network. They also have long histories of experience with each other, contributing to implied norms of confidentiality upon which individuals should be able to rely. Indeed, evidence was admitted at trial that "[a]ll who may have seen the model were intimate friends of [the inventor] and he would have been 'astonished if any of them had felt free to do something with … the idea."[210] What's more, these friends, roommates, and colleagues, some of whom were fellow chemists, were not engineers or puzzle experts: merely showing them a series of cubes with rotating blocks would not have allowed them to reverse engineer the device. Therefore, given the audience's relationship to the subject matter of the invention, the information disclosed was complex and of the type unlikely to be easily transmitted outside the network via weak ties. Social network and trust theory suggest that the inventor's demonstrations were not public.

And *JumpStart v. Jumpking* would, like the court found, result in a finding of public use under privacy as trust. The invention—protective netting around a trampoline[211]—is simple to understand and easy to transmit by the weak ties (neighbors) that used it in the inventor's backyard. Although norms of trust can indeed develop among acquaintances, additional evidence would likely show little basis for trust based on experience or transference. This suggests that the invention could be disseminated to other networks beyond just a few neighbors.

The real power of privacy as trust, though, is evident from the cases where results and reasoning would change, best illustrated by a Cluster B case, *Beachcombers*,[212] and a Cluster A case, *Honeywell*

[209] Moleculon, 793 F.2d at 1266-67.

[210] Moleculon Research Corp. v. CBS, Inc., 594 F. Supp. 1420, 1425 (D. Del. 1984).

[211] JumpSport, 191 Fed. Appx. at 929.

[212] 31 F.3d 1154 (Fed. Cir. 1994).

International v. Universal Avionics Systems.[213] In *Beachcombers*, the Federal Circuit found that demonstration of a new kaleidoscope at the designer's home constituted invalidating public use.[214] The court was not clear about its reasoning; the lack of any analysis may suggest that the court was simply relying on the lack of any confidentiality agreement.[215] At a minimum, it is clear that the court ignored the social context of disclosure. The invite-only party was at the designer's private home gathered 20-30 of her friend and for the express purpose of soliciting feedback.[216] Despite the lack of any formal secrecy agreement, social network and trust theory would conclude that what happened at the cocktail party was not public use. The audience members were her friends, many of whom likely fall into the strong tie category and engender norms of confidentiality; additional evidence could be admitted to describe the audience in more detail. In any event, that those in attendance were the designer's social friends suggests that the technology of the kaleidoscope was relatively complex to them, making it the type of information that does not travel well through weak ties. Therefore, even if the invitees included some acquaintances or weak ties, the details of the invention would be unlikely to travel well from network to network. Nor should we ignore the fact that the alleged public use took place at the designer's home, a paradigmatic private context,[217] which not only makes further information diffusion even less likely, but also contributes to the emergence of reliable norms of confidentiality.

The result in *Honeywell* would also change. That case involved Honeywell's terrain warning system,[218] which help prevent pilots from flying into mountains and which was demonstrated to potential customers and a reporter more than one year before patenting.[219] The Federal Circuit found no public use because all demonstrations could be considered experimental. That rationale rings hollow: the demonstrations were for customers—more than 150 of them[220]—who, the court admitted, would be purchasing the technology in the future.[221] It was more important to the court that Honeywell personnel conducted the demonstrations and "maintained control over them," even though it is hard to imagine who else would be conducting the test runs. To make these demonstrations seem

---

[213] 448 F.3d 982 (Fed. Cir. 2007).

[214] Beachcombers, 31 F.3d at 1160.

[215] *Id.*

[216] *Id.*

[217] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001) ("the interior of homes [is] the prototypical and hence most commonly litigated area of protected privacy").

[218] Honeywell, 488 F.3d at 987.

[219] *Id.* at 998.

[220] Honeywell Int'l, Inc. v. Universal Avionics Sys. Corp., 343 F. Supp. 2d 272, 307-8 (D. Del. 2004).

[221] *Id.* at 308.

relatively private, the district court emphasized that there was no indication that the general public ever became aware of the technology.[222] That a reporter was on board was irrelevant.

Social network and trust theory would conclude, from the totality of the circumstances, that Honeywell engaged in public use. The audience for its disclosure included members of the aviation industry that were likely going to purchase the system and a former pilot and aviation reporter that subsequently wrote an article about the technology. These are precisely the kind of weak ties that could both understand the technology and disseminate it; indeed, the writer's job is to disseminate the information. There is also no indication, unlike, say, in *Bernhardt*,[223] that the norms and customs of the aviation industry ensure that all parties share the burden of keeping information confidential. Additional evidence about industry norms and practice could be admitted to buttress or challenge that conclusion.

There are undoubtedly some closer calls, but additional evidence could help us apply the social network and trust model. In *Lough*, for example, where a boat repairman installed his new device on his friends' boats,[224] we would want to know more about these friends, their history with the inventor, and their proficiency with boat hardware and technology. In *NRDC*, where the inventor's academic adviser disclosed his student's invention to an acquaintance at an academic conference,[225] applying social network and trust theory would require additional evidence on the relationship between the parties. But this type of evidence is easily admitted, the detour into social science well worth the added fairness benefits.

In the end, social network and trust theory offer a fair and administrable approach to public use cases. The proposal resembles trade secrecy's relative secrecy doctrine, brings intellectual property's respect for social networks to a forgotten corner of patent law, and, in so doing, treats corporate and solo inventors equally and gives everyone a chance to contribute to the innovation economy. In some situations, cases would have come to different results under privacy as trust. But for most cases, the doctrine provides a robust intellectual foundation for reasoning through public use questions and helps ensure honest application of what was always meant to be a flexible standard for patent validity.

B. Responses to Potential Objections

---

[222] *Id.*

[223] Bernhardt, L.L.C. v. Collezione Europea USA, Inc., 386 F.3d 1371, 1381 (Fed. Cir. 2004). *See also supra* notes 81-85 and accompanying text.

[224] Lough, 86 F.3d at 1121.

[225] NRDC, 17 F.3d at *3.

Some might object to the structure or mode of analysis of privacy as trust as too indeterminate and inappropriate for patent law. Others might focus on the results, suggesting that the proposal would encourage risky business behavior and cut off more knowledge from the public domain, thus running counter to the goals of patent law. I respond to these objections in turn.

A totality of the circumstances test, one might argue, is too flexible and too indeterminate, providing too much discretion, too few guidelines, and no way to prevent a judge from imposing his personal preferences on a given case. This is a common refrain in divers areas of law,[226] but it rings hollow in this case. Totality of the circumstances tests, in general, allow fair and individual determinations of fact-specific cases. And even under the current standard, public use cases are highly fact specific, depending on the inventor's actions, the details of the disclosure, and whether she had the foresight and leverage to mandate nondisclosure. What's more, the very deficiencies identified in this Article—discriminatory application of public use law to privilege corporate inventors over solo entrepreneurs—stem not from a boundless totality of the circumstances test, but a misapplication of the law through a bright line privacy as control standard.[227] Although bright line rules are undoubtedly more definite, this Article's social network and trust approach comes with clear guidelines that limit the analysis to only relevant factors: the social context of disclosure, the information disclosed, and the relationships between the audience and the inventor and the audience and the information.[228]

---

[226] *See, e.g.*, Barry C. Feld, *Criminalizing Juvenile Justice: Rules of Procedure for the Juvenile Court*, 69 MINN. L. REV. 141, 173-77 (1984) (juvenile criminal justice); WAYNE R. LAFAVE AND JEROLD H. ISRAEL, CRIMINAL PROCEDURE § 3.3, at 143-45 (2d ed. 1992) (determining culpability); B.J. Huey, *Undue Hardship or Undue Burden: Has the Time Finally Arrived for Congress to Discharge Section 523(A)(8) of the Bankruptcy Code?*, 34 TEX. TECH L. REV. 89, 108 (2002) (tax); Samuel Issacharoff, *Polarized Voting and the Political Process: The Transformation of Voting Rights Jurisprudence*, 90 MICH. L. REV. 1833, 1845 (1992) (voting rights). Lough v. Brunswick Corp., 103 F.3d 1517, 1519 (Fed. Cir. 1997) (Lourie, J., concurring) ("With respect to … public use …, courts have been accustomed to referring to their determinations as involving 'the totality of the circumstances,' a phrase that some have objected to as being indefinite."); Seal-Flex, Inc. v. Athletic Track & Court Constr., 98 F.3d 1318, 1323 n.2 (Fed. Cir. 1996) (stating, in the on-sale bar context, that the totality of the circumstances test is often criticized as being unnecessarily vague).

[227] *See supra* notes 48-55 and accompanying text.

[228] Nor has the Federal Circuit disclaimed a totality of the circumstances test in public use cases. Until the Supreme Court decided *Pfaff v. Wells Electronics*, 525 U.S. 55 (1998), the federal courts had been using a totality of the circumstances test to adjudicate both the public use and on-sale bars. *Pfaff*, an on-sale bar case, switches the standard to a "ready for patenting" test, but since the Court had no occasion to address public use, the totality of the circumstances remained for the public use bar. But the Federal Circuit's decision in *SmithKline Beecham Corp. v. Apotex Corp.*, 365 F.3d 1306 (Fed. Cir. 2004), vacated en banc, 403 F.3d 1328 (Fed. Cir.), aff'd on other grounds, 403 F.3d 1331 (Fed. Cir. 2005), opted to apply the

A second structural objection to this Article's social network and trust proposal is that it imports a doctrine from unrelated areas of law and social science that address problems and policies distinct from patent law. I disagree. Not only did Sam Warren and Louis Brandeis refer to the doctrinal and theoretical relationships between intellectual property and privacy law more than 125 years ago,[229] distinguished scholars in both fields have been learning lessons from each other ever since.[230] Indeed, paraphrasing Jonathan Zittrain's powerful argument, the "problem" of privacy and intellectual property is the same: information flow.[231] In privacy, individuals seek to protect the dissemination of personal data; many privacy questions concern the wrongful disclosure of intimate information. The public use bar addresses a similar matter—namely, the diffusion of information about an invention. To answer these questions, both fields seek a way to draw the boundary between public and private after an initial, limited disclosure. Considering similar approaches, therefore, makes sense.

The final two objections concern the practical implications of employing a social network and trust approach to public use. Some might argue that by recognizing the norms of confidentiality of informal relationships between friends and intimates, this Article's proposal would result in more findings of nonpublic use. But allowing more inventors to use their devices without the voluminous disclosures required in a patent application would run counter to the a central goal of patent law, i.e., the disclosure of knowledge to the public.[232] This argument misreads the data and misses the point of privacy as trust. As discussed above, many public and nonpublic use cases would come to same results under a social network and trust approach. The proposal is merely a mode of analysis that also

---

Supreme Court's on-sale rule to public use. Still later, the Federal Circuit appeared to return to a totality of the circumstances test in *Bernhardt v. Collezione Europa*, 386 F.3d 1371 (Fed. Cir. 2004), and in *Dey v. Sunovision*, 715 F.3d 1351 (Fed. Cir. 2013). In *Invitrogen Corp. v. Biocrest Manufacturing, L.P.*, 424 F.3d 1374 (Fed. Cir. 2005), the Federal Circuit offered a middle ground that ultimately retained the totality of the circumstances test for determining public use. The court stated that the "proper test" for public use is "whether the purported use: (1) was accessible to the public; or (2) commercially exploited." That said, determining "publicness" under prong (1) required falling back on the totality of the circumstances test described above. *Id.* at 1380.

[229] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198-205 (1890).

[230] *See, e.g.*, Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201 (2000).

[231] *Id.* at 1203.

[232] Sinclair & Carroll Co. v. Interchemical Corp., 325 U.S. 327, 330-31 (1945) ("[t]he primary purpose of our patent system is not reward of the individual but the advancement of the arts and sciences. Its inducement is directed to disclosure of advances in knowledge which will be beneficial to society; it is not a certificate of merit, but an incentive to disclosure.").

addresses inequality in the application of current public use law. If it does result in more solo entrepreneurs being allowed to retain their patents, so be it: the PTO has already recognized the need to improve access by part-time inventors and hobbyists[233] and the progress of science and technology in society, the salient and overarching purpose of the patent system,[234] could only benefit.

Some may argue, too, that even if secrecy commitments are not always be possible, codifying norms of confidentiality as adequate replacements encourages risky behavior. The law, the argument continues, should incentivize corporate and solo entrepreneurs alike to take every necessary precaution to secure their inventions, and downplaying confidentiality agreements does the opposite. I resist the temptation to use a discriminatory weapon as a paternalistic tool that has a disparate impact on lone inventors. Focusing on the context of disclosure encourages risky behavior no more than privacy law does when it allows individuals to rely on their legitimate expectations of privacy. And the elevation of confidentiality agreements to near determinative status is less a tool of social policy than a give away to corporate entities that have the leverage to employ them. What's more, as evidenced by its Pro Se Assistance Program and Law School Clinic Program,[235] the PTO already believes that solo entrepreneurs deserve a chance to access the innovation economy without having to meet some of the same demands as corporate inventors. A social network and trust model to public use, therefore, does not so much encourage bad behavior as implement an egalitarian approach to patentability.

Conclusion

Current public use law tends to privilege corporate inventors over solo entrepreneurs. It does so by employing a privacy as control model for determining when a pre-patenting disclosure or use was sufficiently public to invalidate a patent, elevating confidentiality agreements to near determinative status, and respecting the confidentiality norms of industry while ignoring the different, yet equally as powerful norms of individuals. This Article proposes a new way of thinking through and adjudicating public use cases by employing a privacy as trust model. This approach recognizes that disclosure is a contextual, fact-specific social phenomenon that can only be evaluated through the lens of social science, specifically social network theory and trust. An administrable model that focuses on the social context of disclosure, the relationship between the inventor

---

[233] *See* Pro Se Assistance Program, at http://www.uspto.gov/patents-getting-started/using-legal-services/pro-se-assistance-program.

[234] Sinclair, 325 U.S. at 330-31. *See also* U.S. Const., art. I, § 8, cl. 8.

[235] Law School Clinic Certification Program, at http://www.uspto.gov/learning-and-resources/ip-policy/public-information-about-practitioners/law-school-clinic-1.

and her audience, and the relationships between the audience and the information disclosure is proposed, as well. As applied, privacy as trust may change results in some cases, but more importantly, it will provide a coherent, predictable, and fair method for analyzing public use cases.

Research into the role of social network theory and trust, in general, and in intellectual property law, specifically, must continue. With respect to public use, this Article has not considered questions of institutional competence, or whether judges or juries are more capable of the social science analysis proposed herein. As for other questions across the intellectual property spectrum, future scholarship will tease out the role of social networks and trust in the publicity triggers in the Copyright Act's exclusive rights. And the importance of trust in other areas of law must be teased out, as project on which several scholars are already engaged. Needless to say, this Article is one step in a larger research project. But when it comes to public use law, social network and trust theory offer a practical, egalitarian, and honest way forward. More work is to come.