

American Law & Economics Association Annual Meetings

Year 2005

Paper 42

A Social Networks Theory of Privacy

Lior J. Strahilevitz
University of Chicago Law School

This working paper site is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the publisher's permission.

<http://law.bepress.com/alea/15th/art42>

Copyright ©2005 by the author.

A Social Networks Theory of Privacy

Lior Jacob Strahilevitz*

I.	Why Protect Privacy?	4
A.	Norms and Law	6
B.	The Goals of the Law	7
C.	Privacy Can Be Objective and Descriptive	11
D.	“Computer Model” versus “Public Opinion”	14
II.	The Law of “Limited Privacy”	16
A.	“Limited Privacy”	17
B.	The Hard-Line Cases	20
III.	Social Network Theory	23
A.	The Strength of Weak Ties	28
B.	Network Structure	32
C.	Cultural and Strategic Considerations in Sharing	33
1.	HIV	34
2.	Girls’ School Gossip	36
3.	Hong Kong Bakeries	37
D.	Interaction Between Structure and Culture	39
E.	Predictive Social Network Analysis	42
F.	Lessons	44
IV.	Reading the Case Law in Light of Social Network Theory	44
A.	Evaluating the Leading Cases	46
B.	Judges or Juries?	50
C.	Institutional Competence	52
D.	Extensions of the Approach	54
V.	Conclusion	56

* Assistant Professor, University of Chicago Law School. Thanks to Amitai Aviram, Emily Buss, Bruce Chapman, Adam Cox, Liz Emens, Richard Epstein, Amitai Etzioni, Ward Farnsworth, Carolyn Frantz, Bernard Harcourt, Ed Iacobucci, Doug Lichtman, Tracey Meares, Bernie Meltzer, Randy Picker, Eric Posner, Richard Posner, Adam Samaha, Paul Schwartz, Dan Solove, James Spindler, Geof Stone, Katherine Strandburg, Cass Sunstein, and Michael Trebilcock for their comments on an earlier draft, and to workshop participants at the University of Chicago, the University of Michigan, and the University of Toronto. Further thanks to Sean Griffin and Andres Vidal for helpful research assistance.

Imagine your deepest, darkest secret – a true, but deeply embarrassing, fact about yourself. Now suppose that you awake one morning to find this secret suddenly revealed to everyone you know, as well as dozens of strangers. Most of us would regard such a turn of events as a personal catastrophe. Given the unappealing nature of this scenario, and the ease with which juicy secrets can spread among people, one might expect that we would play our cards close to our vests, refusing to reveal these embarrassing details to anyone. Yet it is likely that most readers have shared their most embarrassing details with other people: spouses, siblings, parents, best friends, clergy, psychiatrists, co-workers, or perhaps even strangers on Trans-Atlantic flights. Indeed, millions of Americans have shared their most intimate personal details with dozens of strangers, for example, by participating in a twelve-step group or seeking advice in an online chat room. By common parlance, we still consider these facts to be “secrets” even after we have revealed them to a handful of people.

But do they remain secrets for the purposes of U.S. privacy law, such that a plaintiff can recover in tort against someone who discovers them through improper means or publishes them in a newspaper without her consent? If so, at what point does a fact “cross over” from being a “private matter” to a “public matter” whose widespread disclosure does not provide the plaintiff with a cause of action? Can something still be “private” if two people know about it? Five people? A hundred people? When John Kerry and John Edwards were criticized after the recent debates for violating Mary Cheney’s “privacy” by mentioning her sexual orientation – an orientation that thousands of Americans already knew about – were the critics making a coherent claim?¹ Where, in short, is the legal boundary between public and private?

This is *the* fundamental, first-principles question in privacy law, and a necessary element in the two most important privacy torts, public disclosure of private facts and intrusion upon seclusion.² Indeed, although I will focus on the privacy torts in this paper, the question about what information is deemed “private” or “secret” cuts across many

¹ The law’s answer to the Mary Cheney question is “no.” Press accounts had mentioned her sexual orientation long before the debates. *See, e.g.,* Susan Greene, *Gays: Cheney’s Views an Issue – Daughter’s Orientation Seen as Dichotomy*, DENVER POST, July 27, 2000, at A14. Once a fact has been reported in the press, courts hold that it is no longer private, and third parties can disseminate the fact with immunity. *See* Sipple v. Chronicle Publishing Co., 154 Cal.App.3d 1040, 1047-48 (1984). Nevertheless, an influential columnist invoked Cheney’s privacy as a basis for criticizing Kerry and Edwards. *See* William Safire, *The Lowest Blow – The Kerry Campaign Believes Cheney’s Daughter Is ‘Fair Game,’* PITT. POST-GAZETTE, Oct. 19, 2004, at A17 (noting that prior to Senator Edwards’ mention of Mary Cheney’s sexual orientation, “only political junkies knew that a member of the Cheney family serving on the campaign staff was homosexual. The vice president, to show it was no secret or anything his family was ashamed of, had referred to it briefly twice this year, but the news media – respecting family privacy – had properly not made it a big deal. The percentage of voters aware of Mary Cheney’s sexual orientation was tiny.”).

² The public disclosure of private facts tort requires the plaintiff to show that the defendant (a) gave publicity, (b) to a private fact, (c) that is not of legitimate concern to the public, where such disclosure (d) is highly offensive to a reasonable person. RESTATEMENT (SECOND) OF TORTS § 652(D) (1977).

The tort for intrusion upon seclusion requires the plaintiff to show that the defendant (a) intentionally intruded, physically or otherwise, (b) on the solitude or seclusion of another or his private affairs or concerns, (c) in a manner highly offensive to a reasonable person. *Id.*

areas of American law, including the Fourth Amendment, trade secrets, patents, evidence, the constitutional right of information privacy, and the Freedom of Information Act.³

Despite the centrality of this issue, the American courts lack a coherent, consistent methodology for determining whether an individual has a reasonable expectation of privacy in a particular fact that has been shared with one or more persons. Indeed, jurisdictions cannot agree on a framework for resolving these kinds of cases. Hence, Georgia law holds that disclosing sensitive information to dozens of people, and perhaps even tens of thousands of strangers, does not necessarily render information “public” for the purposes of the public disclosure of private facts tort,⁴ but Ohio law governing the same tort holds that a plaintiff’s decision to share sensitive information with three co-workers eviscerates her expectation of privacy in that information.⁵

This paper argues that insights from the emerging literature on information transmission through social networks can help courts develop a more rigorous and objective notion of “privacy” for the purposes of the privacy torts. It argues that privacy tort law should not focus on the abstract, circular, and highly indeterminate question of whether a plaintiff reasonably expected that information about himself would remain “private” after he shared it with one or more persons. Instead, the law should focus on the more objective and satisfying question of what extent of dissemination the plaintiff should have expected to follow his disclosure of that information to others. The goal here is to solidify the “privacy” inquiry as an empirical question, rather than a highly-contested normative matter. Most courts appear to be treating the question as an empirical one presently, but they are tackling the empirical issue in a casual, careless, and confused manner.

The literature that I introduce herein explores the ways that information flows through society. Studying rumor transmission has long been a subject of some interest among sociologists and economists, and a few more recent studies have focused on the dissemination of information about HIV status and other sensitive forms of personal information through an individual’s social circle. Taken as a whole, this literature provides an informative, albeit incomplete, picture of how likely particular information is to spread through any given social network. I will review this literature, discuss some of its implications for privacy law, and then compare these implications to the analysis that courts have conducted in privacy tort cases. I will argue that social network analysis is an indispensable tool for resolving disputes where the parties to a communication disagree about whether the recipient was entitled to share it with others.

This framework has significant implications for privacy law. In order to determine whether a particular fact known by some people will become widely publicized, one needs to know much more than how many people are currently aware of the fact. Rather, one needs to know where, within a social network, this information exists; what types of people have access to it; what the incentives are for subsequent dissemination are; whether the information must be aggregated with other forms of information in order to become pertinent; and what kinds of social norms facilitate or

³ See *infra* notes 235-240.

⁴ *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491 (Ga. 1994); *Zieve v. Hairston*, 598 S.E.2d 25 (Ga. Ct. App. 2004).

⁵ *Fisher v. Ohio Dept. of Rehabilitation & Correction*, 578 N.E.2d 901 (Ohio Ct. Cl. 1988).

constrain subsequent dissemination of the information. Information known by one hundred people might never be disseminated further, but the widespread dissemination of other information known to only two people might be inevitable. The literature on social networks allows us to identify useful generalizations about the ways in which information flows through social networks. Because information spreads in rather predictable ways, and patterns emerge in particular kinds of networks, courts can use these regularities to analyze the *ex ante* likelihood that previously private information will become widely known. Once courts understand how to do that, it becomes relatively simple for them to evaluate whether a particular fact about a plaintiff eventually would have become public if the defendant had not intervened. This is the precisely the inquiry that privacy tort law demands.

Part I briefly explores the theoretical underpinnings of privacy tort law protection. This part establishes a framework for the discussion that follows. Part II describes the common law's treatment of the question of when information that has been disclosed to one or more people might remain private for the purposes of these torts. Part III delves into the literature on social network analysis. It pays particularly close attention to the ways in which network structure and cultural variables can affect the probability that information disclosed to a few people will ultimately become known by the larger community. Part IV uses the insights from this literature to evaluate the accuracy of judicial efforts to assess whether litigants should have expected that information disclosed to a group of people eventually would be disseminated much more widely. As a general matter, courts do a reasonably good job of making these assessments, but there are a few areas in which their intuitions lead them astray. The paper suggests that using insights from social network theory can help courts evaluate privacy in a more accurate and transparent matter. A brief conclusion follows in Part V.

I. Why Protect Privacy?

The types of privacy issues that this paper seeks to resolve are those involving a plaintiff's disclosure of information about himself to a limited number of people. Under one notion of information privacy, information ceases to be private the moment it is shared with a second person. Yet, as the Supreme Court has recognized, such an unsophisticated conception of "privacy" is much too cramped for a society of social beings.⁶ No one's closet is devoid of skeletons. When asked to imagine the most private facts about ourselves, we will typically think of sexual encounters and bodily functions, sensitive medical information, shameful past misdeeds, unfavorable opinions about peers, and knowledge of our fundamental weaknesses and fears. As I suggested at the outset,

⁶ *United States Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster's initial definition, information may be classified as 'private' if it is 'intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public. . . . In sum, the fact that 'an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information.'").

most of us would regard the disclosure of these details to our entire circle of acquaintances, let alone the public at large, as a personal disaster.

At the same time, no one among us has guarded that embarrassing information with maximum diligence. Certain presumptively “private” acts, such as sexual intercourse, necessarily take place in the presence of at least one other person. Other facts might be created in solitude, but remain, by common parlance, “private” even when shared to some extent. We all tell some people about our medical ailments. Virtually everyone feels the need to unburden himself by confessing embarrassing acts to another. Indeed, sharing our most intimate information with those who we expect to keep it secret promotes further friendship and intimacy.⁷ We tend to like people who confide in us, even if we’ve met them recently.⁸ One respected privacy theorist has gone so far as to suggest that “intimate relationships simply could not exist if we did not continue to insist on privacy for them.”⁹ It should not be necessary to highlight the importance of intimacy in human society. Indeed, describing the benefits of intimacy in economic terms, by referring to its enormous positive externalities, in some ways understates its importance. A man or woman without intimates is a shell of a person.

For the individual, sharing information about herself can be helpful even when intimacy is not involved. Although concerns about intimacy provide the strongest justifications for protecting privacy, there are other reasons why society might value privacy as well.¹⁰ Millions of Americans participate in twelve-step programs and support groups, where it has become completely normal to disclose to a score of strangers one’s status as an alcoholic, bulimic, child abuse victim, heroin addict, AIDS sufferer, or

⁷ CHARLES FRIED, AN ANATOMY OF VALUES: PROBLEMS OF PERSONAL AND SOCIAL CHOICE 142 (1970) (“To be friends or lovers persons must be intimate to some degree with each other. Intimacy is the sharing of information about one’s actions, beliefs or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love.”).

⁸ Thomas E. Runge & Richard L. Archer, *Reactions to the Disclosure of Public and Private Self-Information*, 44 SOCIAL PSYCH. Q. 357, 361 (1981); see also Laurel Richardson, *Secrecy and Status: The Social Construction of Forbidden Relationships*, 53 AM. SOCIOLOGICAL REV. 209, 213 (1988) (arguing that disclosure of pertinent information promotes friendship and intimacy).

⁹ Robert S. Gerstein, *Intimacy and Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 265, 265 (Ferdinand David Schoeman ed. 1984) [hereinafter PHILOSOPHICAL DIMENSIONS]; see also CARL D. SCHNEIDER, SHAME, EXPOSURE, AND PRIVACY 42 (1977) (“[I]n the area of personal relationships, such as family, friends, and lovers, where quality is important, privacy is an operative principle. These relationships can’t be sustained with everyone. To function, they depend on an excluding condition. Privacy creates the moral capital that is spent in friendship and intimate relations.”); Charles Fried, *Privacy: A Moral Analysis*, in PHILOSOPHICAL DIMENSIONS, *supra*, at 203, 209 (“In general it is my thesis that in developed social contexts love, friendship, and trust are only possible if persons enjoy and accord to each other a certain measure of privacy.”). As an empirical matter, intimacy does exist in societies that provide little or no legal protections for private information. That said, we should not be legal centralists when evaluating Gerstein and Fried’s claims. This paper essentially equates legal privacy protections with de facto privacy protections that arise via resource constraints on surveillance and impediments to information dissemination. It may well be that in a hypothetical super-Orwellian world of complete surveillance and instantaneous information dissemination, there would be no intimacy among human beings.

¹⁰ For an exploration of the competing values furthered by privacy law, see Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1099-1153 (2002).

gambler.¹¹ Sharing information within these groups can bring the discloser helpful advice, as well as the sometimes substantial psychological relief associated with revealing certain secrets to people the discloser expects to never encounter again.¹² We are, in short, constantly disclosing embarrassing information about ourselves to third parties, yet we often harbor strong subjective expectations of privacy when doing so. By creating causes of action for invasion of privacy, most jurisdictions have determined that the benefits associated with fostering this intimacy justify the costs of constraining communication. In this paper, I assume the correctness of that judgment, notwithstanding the criticisms that have been lodged against privacy tort liability.¹³

A. *Norms and Law*

In the vast majority of situations, the law does not matter much to people who disclose private information about themselves. When we disclose sensitive information to friends, the law generally has little effect on our expectations that these friends will keep the information secret. Rather, we are relying on our friend's good will, an explicit promise of confidentiality, or perhaps on an implicit threat of retribution if the information is disclosed. Where confidentiality is breached, we might retaliate by refusing to share information with that person in the future, cutting off friendship ties, or disclosing to third parties sensitive information that the loudmouth previously shared with us. A different dynamic arises when we disclose information to strangers. Here, we are relying on obscurity – our own anonymity or the removal of the stranger from our ordinary social circle – to protect the confidentiality of the information. In both settings, however, tort law probably does little to shape people's actual expectations of privacy.

There is, however, a category of sensitive information disclosure that is harmful enough to warrant the imposition of legal liability. These instances generally involve cases of substantial damage to the plaintiff and very widespread publicity.¹⁴ They also tend to involve non-repeat-player relationships between the litigants, perhaps

¹¹ See Jaimie Wilson, *United – By Addiction*, FLA. TIMES-UNION, Mar. 20, 2001, at C1 (noting that Alcoholics Anonymous alone has 1.16 million members in the U.S.); see also James Rachels, *Why Privacy Is Important*, in PHILOSOPHICAL DIMENSIONS, *supra* note 9, at 290, 295 (“Resistance to . . . group therapy is overcome when the patients begin to think of each other not as strangers but as *fellow members of the group*. The definition of a kind of relation between them makes possible frank and intimate conversation which would have been totally out of place when they were merely strangers.”). For a discussion of the importance of twelve-step support groups in American society, and an argument for extending an evidentiary privilege to communications among participants, see Thomas J. Reed, *Compulsory Disclosure of Confidential Communications Among Alcoholics Anonymous Members*, 70 ST. JOHN'S L. REV. 693 (1996).

¹² ALAN F. WESTIN, *PRIVACY AND FREEDOM* 34-36 (1967).

¹³ See, e.g., Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

¹⁴ As a general matter, filing a lawsuit for public disclosure of private facts either introduces those facts into the public record or draws substantial press and public attention to those facts. For a plaintiff who wishes to suppress private information that another person has discovered, filing suit is often a very poor strategy. We can therefore expect that invasion of privacy disputes will be filed when the plaintiff has little left to lose from further publicity.

characterized by substantial power disparities, such that reputational sanctions often will not deter the conduct in question, and the plaintiff has no effective way of engaging in self help. Indeed, the typical invasion of privacy case involves a media defendant.¹⁵ Unlike the people who disclose information about themselves to each other, these would-be defendants are playing close attention to the law.

It is through the regulation of these legally sophisticated parties that tort law may have a strong, albeit indirect, effect on ordinary people's expectations of privacy. Ordinary people will expect little privacy in a world where sensitive information about private figures that does not appear to have been extracted and disseminated with the subjects' consent regularly appears on television and in newspapers. Because people understand that there is often an intermediate actor between the subject of the report and the reporter, they will become more reluctant to share information about themselves as information about others, similarly situated, appears with increasing regularity in the mass media.¹⁶ The more ordinary love letters wind up in the *New York Times*, the more guarded private figures composing such letters will become in writing and sending them. All of this poses a real threat to human intimacy, especially for people who overreact to very low probability, but high visibility, reputational harms.¹⁷ A society interested in fostering intimacy should help people disregard these very low probability events.

Tort law can thus function as a form of social insurance: protecting those people who engaged in socially desirable sharing of personal information, but who had the misfortune to see those personal details disseminated to the general public without their consent.¹⁸ Where a large group of similarly situated people share information about themselves, but the news media publicizes only a small percentage of that information, it can be efficient and just for disseminators to compensate the unlucky few.

B. *The Goals of the Law*

Tort liability for public disclosure of private facts attempts to strike a difficult balance by regulating interpersonal communication in a manner that enhances social welfare. On one hand, the law seeks to encourage the expressive and psychological benefits that people derive from disclosing sensitive information about themselves to

¹⁵ Obviously, deep pockets provides a partial explanation for this as well. In some of these cases, there will be an intermediate discloser who is not a party to the suit – e.g., a friend who has blabbed to a reporter.

¹⁶ The relationship I am describing, of course, is non-linear. There may be a tipping point at which sensitive information about individuals becomes so widely disseminated in the media that any stigma attached to the disclosure will wither. This is arguably what has begun to happen in recent years with respect to the disclosure of information about individuals' homosexuality. In such circumstances, we might expect more disclosure of such information within social circles. By the same token, however, as the stigma is diminished, we can expect that the disclosure of the destigmatized information will generate less intimacy between the discloser and discloser and fewer psychological benefits for the discloser.

¹⁷ For a provocative discussion of this issue, see Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999).

¹⁸ For a related argument, see Shubha Ghosh & Vikram Mangalmurti, A Social Insurance Perspective on Security and Privacy (unpublished working paper July 27, 2004), available on ssrn.com.

others. It fosters the kinds of disclosures that lead to intimate relationships, often benefiting both parties to a sensitive communication.

On the other hand, the law seeks to regulate the further dissemination of this information. My subsequent dissemination of secrets that someone has confided in me can be beneficial. Most importantly, it promotes the development of a relationship between me and the person with whom I am sharing the information.¹⁹ Note, however, that sharing private information about someone else seems unlikely to foster as much intimacy as sharing private information about one's self.²⁰

Subsequent dissemination can also help the public understand existing social norms.²¹ Indeed, gossip is often central in theories of social norm enforcement and change.²² Of course, there will be cases where third parties who are kept in the dark stand to gain substantially from learning information that someone else wants to guard. For example, it may make society better off if a third party tells the faithful husband of an adulterous wife about her dalliances. For these reasons, spreading private information about others sometimes benefits society. The tort for public disclosure of private facts therefore limits liability to defendants who (1) publicize information that is (2) private; (3) not of legitimate concern to the public; and (4) disseminated in a highly offensive manner.²³ The first limitation helps keep instances of minor disclosure out of court, by requiring that the defendant spread the information to a large number of people or, in some states, a smaller number of people who have a special relationship with the subject of that disclosure. The third limitation protects First Amendment interests and

¹⁹ ALLAN J. KIMMEL, RUMORS AND RUMOR CONTROL: A MANAGER'S GUIDE TO UNDERSTANDING AND COMBATTING RUMORS 111 (2004); Diego Gambetta, *Godfather's Gossip*, 35 ARCHIVES EUROPEAN SOCIOLOGY 199, 216 (1994).

²⁰ Simply put, trusting someone with one's own secrets makes one vulnerable in a way that sharing someone else's secrets does not. This vulnerability is an ingredient of intimacy. The relationship between gossip and trust is less susceptible to categorical characterizations. See *id.* ("If I confide my secrets to you this may encourage you to trust me and, in turn, to confide more secrets to me. . . . On the other hand, trust increases the likelihood of revealing personal secrets to others and thereby increases the exposure to gossip by increasing the circulation of material suitable for it: if you tell me in confidence a secret about yourself I can pass it on to someone else and breach your trust. If we join the two effects together we find that gossip ultimately should generate *positional* trust: it increases mutual trust among gossiping agents at the costs of breaching trust with those who are the object of gossip. The overall effect on the amount of trust, however, is not clear.").

²¹ Ronald S. Burt, *Bandwidth and Echo: Trust, Information, and Gossip in Social Networks*, in NETWORKS AND MARKETS 30, 46 (James E. Rauch & Alessandra Casella eds. 2001); Donna Eder & Janet Lynne Enke, *The Structure of Gossip: Opportunities and Constraints on Collective Expression Among Adolescents*, 56 AM. SOCIOLOGICAL REV. 494, 494-95 (1991); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 334-35 (1983). In light of subsequent legal developments, the eulogy suggested by Zimmerman's title proved premature. See Patrick J. McNulty, *The Public Disclosure of Private Facts: There is Life After Florida Star*, 50 DRAKE L. REV. 93 (2001); John A. Jurata, Jr., Comment, *The Tort that Refuses to Go Away: The Subtle Reemergence of Public Disclosure of Private Facts*, 36 SAN DIEGO L. REV. 489 (1999).

²² See, e.g., ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 57-59, 79-80 (1991); see also KIMMEL, *supra* note 19, at 85 (arguing that gossip makes social groups more cohesive).

²³ See *supra* note 2.

immunizes those who spread information that has substantial social value.²⁴ The fourth limitation helps ensure that run-of-the-mill information dissemination is not penalized and that relatively unobjectionable breaches of confidentiality do not clog the courts. But what purpose does the second limitation serve?

In my view, tort law's public-private distinction furthers three primary purposes: First, it grants the parties latitude to structure the disclosure of information in a manner that furthers both parties' perceived interests. If people really want to share the most intimate details about their sex lives on the *Jerry Springer Show*, the law lets them do so.²⁵ This is why there is no such thing as inherently private information: In a nation where reality television and blogging are all the rage, it is impossible to find a type of personal fact that no one has shared with thousands of strangers. The law sensibly avoids paternalism and defers to an individual's explicitly articulated decisions to publicize information about himself, reasoning that he is in a better position than the government to weigh the private benefits and costs of this information dissemination and that the costs associated with government intervention here usually exceed the associated social benefits.²⁶ Deciding whether a disclosure was consensual thus plays a pivotal role in determinations of whether particular facts are private.²⁷ For this reason, information

²⁴ Cf. KIM LANE SCHEPPLE, *LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW* 260 (1988) ("[P]rivacy is not allowed when the information has been judged necessary for someone else to know in order to make decisions that she is entitled to make."). The legal determination of "legitimate concern to the public" necessitates paternalistic judgments by judges about what forms of information the public should receive and what forms of information it should not receive. Even if there is great consumer demand for an unauthorized videotape of a celebrity engaged in sexual intercourse, this does not necessarily, and in my view should not necessarily, render the information of "legitimate concern to the public." See *infra* note 195. The presence of paternalistic judgments does not render information privacy law anti-welfarist, but it does indicate judicial skepticism about whether market demand is an accurate proxy for welfare. For a critique of privacy tort law on welfarist grounds, see Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978).

²⁵ The law's deference to individuals' decisions stems from a belief that individuals are in a better position than government officials to make decisions about sharing personal information. That said, my analysis in this section suggests that there may be negative externalities associated with an individual's voluntary disclosure of personal information about herself in circumstances where that consent is not obvious to those who hear the voluntarily disclosed information. It may be appropriate, therefore, for the law to require that viewers, listeners, and readers be exposed to evidence of the subject's consent in those cases where media outlets disseminate previously private information about individuals.

²⁶ Exceptions arise for a few categories of private speech. For example, the criminal law prohibits adults from sharing with minors information relating to their own sexuality. See *John D. v. Dep't of Social Serv.*, 744 N.E.2d 659 (Mass. App. Ct. 2001) (holding that a stepfather's repeated nudity in the presence of his teenaged daughter, combined with other sexual communications, constituted child abuse, notwithstanding the lack of physical contact between the daughter and stepfather). These laws might also be couched as protecting consent, however, because the minors participating in these conversations would be unable to consent effectively to participate in these conversations and be exposed prematurely to highly charged sexual content.

²⁷ SCHEPPLE, *supra* note 24, at 199-200, 203. The leading case for this proposition is *Daily Times Democrat v. Graham*, 162 So.2d 474 (Ala. 1964). For a discussion of consent as a defense in privacy tort cases, see William L. Prosser, *Privacy: A Legal Analysis*, in *PHILOSOPHICAL DIMENSIONS*, *supra* note 9, at 104, 123.

Under the view laid out in this paper, consent is often a decisive consideration in privacy cases. That said, it is unrealistic to expect that people will always reach formal agreements regarding subsequent

disclosed to another person under false pretenses that reasonably suggest confidentiality usually retains its status as private information.

Second, the privacy element of the tort seeks to differentiate between those facts whose disclosure promotes intimacy and those that do not. If I share information with you that is widely known and readily discoverable, that disclosure is unlikely to promote intimacy between us. The law of privacy therefore does not bother to offer these kinds of disclosures legal protection. Rather, the law protects only information that is secret enough so that its disclosure might foster the development of meaningful social bonds.

That said, secrecy is not a sufficient condition for promoting intimacy. Hardly anyone knows my shoe size. But my informing you that I typically wear a 9 ½ does nothing to bring us closer. Intimacy depends on not only secrecy or obscurity, but also on content. That is where the “privacy” element and the “highly offensive to a reasonable person” element of the privacy torts work together. Because of the privacy element of the tort, outing a closeted homosexual may be tortious,²⁸ but outing Mary Cheney is not. Because of the “highly offensive” element of the tort, publishing the closeted homosexual’s shoe size is not tortious, but revealing his sexual orientation may be. Where both elements are satisfied, we can be reasonably certain that the plaintiff’s initial disclosure of the information had the potential to promote intimacy. By trusting someone else enough to share information with him that is both obscure and sensitive, an individual attempts to enhance the intimacy associated with their relationship.

Third, the privacy element helps courts evaluate causation in the torts context. In order to discern whether the defendant has caused the plaintiff’s injury, we need to know whether the plaintiff would have been injured in the absence of the defendant’s intervention.²⁹ This causal question is contained within the doctrinal inquiry of whether the plaintiff has a reasonable expectation that the information at issue would not be disseminated widely. To say that such an expectation of privacy would have been unreasonable is to say that there was a high risk of widespread dissemination regardless of what any particular individual did with the information.

dissemination in cases involving the disclosure of sensitive information. Litigated privacy cases frequently involve legally unsophisticated plaintiffs, and the sharing of confidential information is so common, and so central to society’s flourishing, that formalizing all such disclosures via binding contracts would be foolhardy. Many of the social interactions that provide the facts for privacy law’s leading cases involve non-repeat players, and highly improbable or surprising turns of events. The transaction costs associated with preventing these controversies via contracts often will be prohibitive. In such cases, reasonable expectations of privacy help “fill in the blanks” of a contract that the parties to a communication would have agreed to, had they been able to do so costlessly.

²⁸ See Barbara Moretti, *Outing: Justifiable or Unwarranted Invasion of Privacy? The Private Facts Tort as a Remedy for Disclosures of Sexual Orientations*, 11 CARDOZO ARTS & ENT. L.J. 857 (1993); John P. Elwood, Note, *Outing Privacy, and the First Amendment*, 102 YALE L.J. 747 (1992); Keith J. Hilzendeger, Comment, *Unreasonable Publicity: How Well Does Tort Law Protect the Unwarranted Disclosure of a Person’s HIV-Positive Status?*, 35 ARIZ. ST. L.J. 187 (2003).

²⁹ Causation is not, in and of itself, an element in the public disclosure tort. See, e.g., *Johnson v. Sawyer*, 4 F.3d 369, 382 n.69 (5th Cir. 1993), *rev’d on other grounds*, 47 F.3d 716 (5th Cir. 1995) (en banc). At the same time, my discussion of the case law in Part Two will show that when courts encounter privacy cases involving the plaintiff’s disclosure of information to one or more people other than the defendant, they tend to analyze the “reasonable expectation of privacy” element in a manner similar to the way in which a tort lawyer would understand but-for causation, asking whether the plaintiff’s injury would have occurred in the absence of the defendant’s involvement.

C. *Privacy Can Be Objective and Descriptive*

Given the functions of privacy law, one can imagine several paths that courts might take to demarcate the boundaries between public and private. The first fork in the road raises the question of whether courts should define the privacy element on the basis of a normative inquiry or a descriptive inquiry. Judges taking a normative tack might regard information about medical conditions, sexual orientations, and political affiliations as inherently private, and information about child-rearing attitudes, movie rentals, and Internet chat room activities as inherently public. But such a normative approach immediately encounters serious difficulties. First, individuals and communities will disagree substantially about what information is more private and what is more public. Some homosexuals are closeted and hope to remain so, but are happy to share information about what movies they've rented. Some people are quiet open about their sexual preferences, but zealously avoid discussing their political or religious beliefs with others. Judges represent an elite segment of society, and there is a real danger that the standards of propriety that they introduce into the law will clash with attitudes that reflect changing cultural beliefs and varied preferences among the citizenry.³⁰ Second, normative disagreements about what is or is not private may be impossible to resolve. People starting with different cultural priors, based on age, race, religion, or economic class, will reach very different conclusions about the morality of collecting or publishing information about activities that a plaintiff would prefer to keep private. Was it morally permissible for Senator Kerry to mention the sexual orientation of Vice President Cheney's daughter during the final 2004 presidential debate? There is no objectively correct answer to this question,³¹ and any effort to ground an answer in neutral principles,

³⁰ Privacy is highly responsive to changes in technologies or social norms. Privacy law ought to reflect democratic sentiments, not fight them. It would thus be a substantial mistake to embed in the law the expectations of privacy that prevailed in one era, one society, or one court's opinion. As Al Alschuler has noted in the Fourth Amendment context, "for a judge to elevate his personal visions of privacy above those of the rest of society would be arrogant and inconsistent with appropriate concepts of judicial restraint. A test of constitutional protection that looks to changing cultural sentiments may raise the specter of adjudication by Gallup poll; but idiosyncratic judicial concepts of natural justice – visions, for example, of an inherent human need for privacy at odds with the visions prevalent in society – would have less claim to respect." Albert W. Alschuler, *Interpersonal Privacy and the Fourth Amendment*, 4 N. ILL. U. L. REV. 1, 7 n.12 (1983-84).

Any normative framework regarding what should or should not remain private will be highly contestable, which strengthens the case for privileging the descriptive as the normative, as this paper does. Of course, one needs some normative principle for determining that privacy is worth protecting. *See supra* Sections I.A. & I.B. That said, the structure of the privacy torts already makes normative considerations relevant. An actionable public disclosure or intrusion must be "highly offensive to a reasonable person." Given that a violation of community standards is a necessary, normative, element of the tort, there is little justification for making the separate "privacy" element turn on normative calculations. This is another reason why I advocate a positivist approach to privacy in this paper.

³¹ Compare Editorial, *Outing Mary Cheney*, WALL ST. J., Oct. 15, 2004, at A14 ("By outing Mary Cheney before millions of viewers on prime-time television, Messrs. Kerry and Edwards may hope to score points with their base of gay activists."), with Brian Lehrer, Editorial, *They'll Point Fingers but Won't Show Their Hands – With the Media's Complicity, Candidates Attack Opponents and Avoid Discussing Ideas*, NEWARK STAR-LEDGER, at 15 ("The Bush campaign is trying to focus voter attention on the fact that John Kerry mentioned in the last debate that Dick Cheney's daughter is a lesbian. This takes the focus off the real

other than popular beliefs or behaviors, is doomed.³² Perhaps because normative analysis leads to dead ends with respect to whether information is appropriately characterized as private or public, most courts view the “privacy” determination in tort law as a descriptive question.

None of this suggests that there is no role for normative analysis in privacy law. I actually want to make a narrower claim than that. Two of the elements of the public disclosure tort are inherently normative – elements 3 (not of legitimate public concern), and 4 (highly offensive to a reasonable person) – but the other two, elements 1 (publicity) and 2 (privacy), are properly understood in purely descriptive terms. For the intrusion tort, element 3 (highly offensive to a reasonable person) is normative, but elements 1 (intentional intrusion) and 2 (private affairs or concerns) are descriptive. So when I say that privacy the “element” should be understood purely descriptively, I do *not* mean that privacy the “concept” should be a purely descriptive inquiry. The concept demands both normative and descriptive inquiries.

Once a court decides to treat the question of whether the privacy *element* is satisfied as a descriptive one, it reaches the second fork in the road, which implicates the subjective-objective distinction. The courts might ask what the parties *actually* expected when the plaintiff’s initial disclosure occurred. Or they might examine what the parties reasonably *should have* expected at the time of the initial disclosure. For very good reasons, courts have focused on the latter inquiry. It seems daft to render the defendant liable for breaching a plaintiff’s unrealistic or foolhardy expectations of privacy. Moreover, evaluating the parties’ subjective expectations of privacy requires the courts to try to get inside the parties’ minds, and parties will often have strong incentives to lie or otherwise shade their recollections about what they expected. As explained below, many litigated privacy disputes will involve cases where the plaintiff apparently expected that the disclosed information would remain private, but the defendant believed that the plaintiff had no such expectation.³³ For that reason, tort opinions have eschewed a

issue of what legal rights gay people should have and puts it on the fake issue of whether Kerry invaded the privacy of someone who is already out and who was already an issue in the campaign.”); *see also supra* note 1.

³² For a fuller and more provocative exploration of these themes, see Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change*, 80 CAL. L. REV. 1133, 1159-62 (1992). Bezanson and I part ways, however, in that he believes that social norms have broken down with respect to the communication of sensitive information, while I believe that empirical studies of communication identify widely held norms and regularities.

³³ In this sense, privacy tort law is quite different from Fourth Amendment law, which ostensibly requires a court to examine *both* subjective and objective expectations of privacy. The courts first ask whether the defendant had a subjective expectation of privacy, and if so, courts examine whether that expectation of privacy is one that society ought to recognize as reasonable. *Katz v. United States*, 389 U.S. 347 (1967). As a practical matter, however, defendants virtually always claim to have a subjective expectation of privacy, and the courts rarely second-guess those representations about the defendant’s state of mind. When courts do discuss the first-prong, their analysis sometimes invokes the “reasonableness” issues that ought to be analyzed under the second prong. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 742-43 (1979) (discussing the issue of whether telephone subscribers in general expect privacy in the numbers that they dial but, strangely, considering this question as part of prong 1 of *Katz*). The second prong of *Katz*, the so-called objective prong, is therefore the locus of most of the action under Fourth Amendment law. *See, e.g., James J. Tomkovicz, Beyond Secrecy for Secrecy’s Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 653-54, 679-80 (1985); David W. Cunis, Note,

subjective inquiry into the parties' states of mind, and focused exclusively on whether the parties' should have expected dissemination or not.

This brings us to the final fork in the road. How might the courts decide whether the parties' privacy expectations (or lack thereof) were reasonable, particularly where those expectations differed substantially? Here again, there are at least two options in cases where the plaintiff and defendant differed about whether they expected subsequent dissemination to occur. The court can ask what most people would have believed, given the context of the initial disclosure. Or the court can ask about the probability that the information at issue would have become public anyway in the absence of the defendant's actions. As a theoretical matter, you could answer the first question by taking a public opinion poll and the second question by modeling the network of communicants to determine whether any dissemination that did occur was likely or a mere fluke. The ideal answer to the second inquiry would employ a sophisticated computer model that perfectly reflects social tendencies, and predicts the *ex ante* likelihood that information disclosed from *A* to *B* will ultimately become widely known in the relevant community. If dissemination was likely or inevitable, then the plaintiff's expectation of privacy at the time of the disclosure was unreasonable. If dissemination was highly unlikely, then it was reasonable for the plaintiff to expect privacy.

Courts resolving privacy cases have decided to pursue the "computer model" line of inquiry, ignoring the "public opinion" approach to privacy. Unfortunately, they have done so without the benefit of any obvious methodology, let alone the hypothetically perfect predictive computer model I described in the previous paragraph. Lacking both a computer model and an understanding of the science of social network analysis, judges have relied on their intuitions to evaluate the likelihood of information dissemination in a counterfactual world. Judges seem to be asking themselves, "had the defendant not become involved, would I have expected this information to remain private were I in the parties' shoes?" I have suggested that this is the right question to be asking. But the answers that courts have provided seem to rely on guesswork more than anything else. We can use sociology to assess the accuracy of judges' guesses, and perhaps to help them

California v. Greenwood: *Discarding the Traditional Approach to the Search and Seizure of Garbage*, 38 CATH. U. L. REV. 543, 565 (1989); Jon E. Lemole, Note, *From Katz to Greenwood: Abandonment Gets Recycled from the Trash Pile – Can Our Garbage Be Saved from the Court's Rummage Hands?*, 41 CASE W. RES. L. REV. 581, 590 n.92 & 601 (1991).

Two other differences are worth noting here. First, in the Fourth Amendment context, the law deems the government agents' expectations of the plaintiff's privacy irrelevant. Rather, the law focuses only on what the subject of the search expected, and whether those expectations were reasonable. In the privacy tort context, by contrast, both parties' expectations might be relevant. Before assigning civil liability to a defendant, a court might want to know whether the defendant expected that the information in question was supposed to remain private. Second, in the Fourth Amendment context, the federal courts have adopted a version of what I call the hard-line approach to privacy. If an individual discloses information with a third party, that information is deemed to have been disclosed to the entire world. See *infra* Section II.B. and note 235. For criticisms of existing Fourth Amendment jurisprudence, and arguments on behalf of "privacy in public," see Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349 (2004), and Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002).

make better educated guesses.³⁴ Before we do that, it makes sense to discuss why the “computer model” approach is preferable to the “public opinion” approach in the tort context.

D. “Computer Model” versus “Public Opinion”

There is, perhaps, an easy explanation for why courts have not considered using a public opinion poll to resolve privacy tort disputes: No scholar has suggested that they do so. But Christopher Slobogin and Joseph Schumacher have argued, quite forcefully, that public opinion polls ought to be relevant to the courts as they decide whether the subject of a government search had a “reasonable expectation of privacy” that is protected by the Fourth Amendment.³⁵ It is not a large leap to apply Slobogin and Schumacher’s Fourth Amendment arguments in the tort context.

That said, in the tort context, making poll data decisive on the privacy question might be ill-advised. Whatever the merits of Slobogin and Schumacher’s proposal as applied to searches and seizures, it is not clear why it matters whether most people say they expect privacy in a particular setting. If large majorities of the American public tell pollsters that “what happens in Vegas stays in Vegas,” this need not make the supposition a reasonable one. To the contrary, it seems that courts would want to base substantive privacy law protections, not on what people say, but on what they do. Thus the courts may properly inquire whether it was appropriate for the defendant (and many other people like him) to believe that a particular disclosure would not be disseminated widely.

Imagine a plausible situation where poll results deviate substantially from actual, observed behavior. For example, assume that 80% of respondents say that if they found out about a friend’s extramarital affair, they would tell that person’s spouse. Now assume that only 20% of people who find out about such affairs actually *do inform* the affected spouses.³⁶ Such a conflict makes the choice of “computer model” versus “public opinion” matter, and whereas the poll probably reflects people’s aspirations (about what they should do), the behavioral study reflects actual data about what is likely to happen. People are social beings. They spend their entire lives disclosing information about themselves and then seeing whether that information remains confidential or spreads through their circles of acquaintances. To the extent that intelligent individuals are

³⁴ Alschuler, *supra* note 30, at 8 n.12 (describing the dictate of *Katz v. United States* that judges “assume the role of armchair sociologists and attempt to assess cultural expectations of privacy” for purposes of Fourth Amendment law).

³⁵ Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at “Understandings Recognized and Permitted by Society,”* 42 DUKE L.J. 727 (1993); Slobogin, *supra* note 33, at 263-75.

³⁶ Divergences between poll results and behavioral data are common in the information privacy context. For an interesting discussion of these divergences and how they might be interpreted, see Katherine J. Strandburg, *Too Much Information: Privacy, Rationality, Temptation and the Implications of “Willpower” Norms* 8-13 (unpublished manuscript on file with author) (2004). Similar divergences between polling and observation arise in the family law context. Fiancées who are aware of high American divorce rates nevertheless assume that their own marriages will not end in divorce. See generally Lynn A. Baker & Robert E. Emery, *When Every Relationship is Above Average: Perceptions and Expectations of Divorce at the Time of Marriage*, 17 LAW & HUM. BEHAV. 439, 443 (1993).

gauging whether information they share with third parties will be shared further, they will focus on observed behavior, not attitudes. Behavioral data is thus preferable to survey data in privacy, just as reliable market data is preferable to contingent valuation data in the realm of environmental law.³⁷

A “public opinion” standard for evaluating reasonable expectations of privacy would create other problems as well. For one thing, such a standard necessarily introduces circularity into the law. A well publicized Supreme Court opinion holding that people have a reasonable expectation of privacy against the use of infrared cameras to detect heat emanating from their homes³⁸ presumably will increase the percentage of poll respondents who view such searches as unduly intrusive. Indeed, the Supreme Court has expressed substantial uneasiness about the possible circularity between people’s expectations of privacy and the content of privacy law.³⁹ What’s more, poll responses can be manipulated rather easily based on the way in which a particular question is framed.⁴⁰ Slobogin & Schumacher point out that their poll results will vary dramatically based on the subject of the search, whether the search revealed anything, and whether the poll respondent is asked about a search of himself or a search of a third party.⁴¹ And, indeed, polling is more uniform in the Fourth Amendment context, where all fact patterns necessarily involve police surveillance. In the tort context, the public’s reaction to a possible privacy invasion will depend heavily on the identities of the parties, the extent of the disclosure, the purpose of the disclosure, the nature of the information disclosed, and various other facts.

The case for “computer model” data over “public opinion” data, then, hinges largely on the law’s preference for observational data over survey data. A complete defense of computer modeling should invoke two additional points. First, jury sentiment may be a decent proxy for localized public opinion polls, substantially reducing the value

³⁷ See Note, “Ask a Silly Question . . .”: *Contingent Valuation of Natural Resource Damages*, 105 HARV. L. REV. 1981 (1992).

³⁸ *Kyllo v. United States*, 533 U.S. 27 (2001).

³⁹ See *Smith v. Maryland*, 442 U.S. 735, 741 n.5 (1979) (“Situations can be imagined, of course, in which Katz’s two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects.”).

Some have criticized the Supreme Court’s Fourth Amendment jurisprudence for facilitating the incremental erosion of people’s privacy expectations. See, e.g., Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843 (2002). This does not strike me as a particularly persuasive critique of privacy law. Rather, the advantage of the reasonable expectations of privacy approach is its flexibility and responsiveness to technological and social changes that affect privacy norms. In any event, a theory of privacy grounded in a social-network theory / computer model approach will be responsive to technological changes as well.

⁴⁰ See, e.g., John Zaller & Stanley Feldman, *A Simple Theory of Survey Response: Answering Questions Versus Revealing Preferences*, 36 AM. J. POLI. SCI. 579 (1992); Lee Anne Fennell, *Death, Taxes, and Cognition*, 81 N.C. L. REV. 567, 594-95 (2003).

⁴¹ Slobogin & Schumacher, *supra* note 35, at 762-64. For another report on the results of national polls dealing with privacy matters, and how responses have varied over time, see James E. Katz & Annette R. Tassone, *The Polls – A Report: Public Opinion Trends: Privacy and Information Technology*, 54 PUB. OP. Q. 125 (1990).

added by survey research. Second, in defamation cases that involve privacy interests, the courts have long relied on a methodology that is analytically similar to computer modeling. In cases involving private figures or non-newsworthy events, defamation law focuses on the truth or falsity of the defendant's statement.⁴² The law does not focus on whether the defendant expected that the information at issue was true, but on whether it actually was true. A newspaper that publishes a false story about a private figure may be liable, even if the newspaper reasonably believed the story to be true at the time of publication. As a result, the newspaper has a strong incentive to evaluate the story's accuracy before publishing it. Evaluating privacy is no more difficult for a would-be defendant than evaluating truth, and in some cases it will be easier. And successful privacy claims, particularly those involving public disclosure of private facts, necessarily involve non-newsworthy facts and often involve private-figure plaintiffs. The analog to defamation law, where expectations are irrelevant as to liability for private figure plaintiffs, even if those expectations are widely held, therefore buttresses the case for a "computer model" approach.⁴³

It remains to be seen whether the "computer model" approach to tort privacy is workable for resource-constrained courts. The answer to that question depends, of course, on the state of the science, so this paper will evaluate that important question in great detail. To foreshadow a bit, the models developed by social network theorists are becoming increasingly sophisticated at predicting whether information will be disseminated widely through a given community. Though their models remain far from perfect, there are already enough useful insights to render social network theory a superior alternative to public opinion polls for evaluating the parties' reasonable expectations of privacy. Before reaching that section of the paper, I will make the discussion more concrete by describing the tort law in some detail.

II. The Law of "Limited Privacy"

The American law eschews a categorical answer to the question of under what circumstances a limited disclosure of private information about one's self renders that information "public" for the purposes of tort law. Puzzlingly, little legal scholarship has addressed this central issue of privacy law.⁴⁴

⁴² See *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974) (holding that private figure plaintiffs need not demonstrate actual malice to recover compensatory damages); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749 (1985) (holding that a plaintiff need not demonstrate actual malice to recover compensatory damages if the speech at issue does not involve a matter of public concern).

⁴³ Nor does trade secrets law consider the parties' expectations to be a substantial factor in whether a valuable commercial idea has been shared so widely to have lost its status as a trade secret. See *Rockwell Graphic Sys. v. DEV Indus.*, 925 F.2d 174 (7th Cir. 1991).

⁴⁴ For a notable exception, see Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1664-70 (1999) (embracing a limited privacy vision of the law, and discussing it in several privacy law contexts).

A. “Limited Privacy”

Privacy law is better developed in California than in any other U.S. jurisdiction, and it appears that California has most emphatically accepted the concept of limited privacy. “Limited privacy” is the idea that when an individual reveals private information about herself to one or more persons, she may retain a reasonable expectation that the recipients of the information will not disseminate it further.

The leading California case is the supreme court’s 1999 opinion, *Sanders v. ABC*.⁴⁵ *Sanders* involved the efforts of Stacy Lescht, an ABC investigative journalist, to expose fraud in the telephone psychic industry. To that end, she obtained employment as a telephone psychic, and used a hidden video camera to record her conversations with co-workers.⁴⁶ One of these co-workers, Mark Sanders, sued after part of his conversation with Lescht was broadcast on ABC’s *PrimeTime Live* program.⁴⁷ Lescht argued that because Sanders’ co-workers could overhear her conversations with him, he had no reasonable expectation of privacy in the communication.⁴⁸ The court disagreed:

This case squarely raises the question of an expectation of limited privacy . . . [P]rivacy for the purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law. . . . “The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone.”⁴⁹

The court thus held that information can be *public* vis-à-vis one’s fellow employees, but *private* vis-à-vis the outside world. Sanders presumably would have suffered little damage if Lescht had played their recorded conversations for fellow employees, but he had a cause of action when she exposed millions of television viewers to the contents of the conversations. Following a jury trial, Sanders was awarded \$635,000 for intrusion upon seclusion.⁵⁰ In other interesting contexts, the California courts generally have adhered to the “expectation of limited privacy” approach laid out in *Sanders*.⁵¹

⁴⁵ 20 Cal. 4th 907 (1999).

⁴⁶ *Id.* at 910.

⁴⁷ *Id.* at 913 n.1.

⁴⁸ *Id.* at 917-18. Approximately telephone psychics worked at cubicles in a large room. *Id.* at 912.

⁴⁹ *Sanders*, 20 Cal.4th at 915-16 (quoting 1 MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY (1998) § 5.10[A][2]).

⁵⁰ *Id.* at 912-13.

⁵¹ See *M.G. v. Time Warner*, 89 Cal.App.4th at 623 (2001) (holding that little league players and coaches had a reasonable expectation of privacy in their team photo, after Sports Illustrated published the photo in a story about the team manager’s molestation of several team members); *Pettus v. Cole*, 49 Cal.App. 4th 402, 441-43 (1996) (holding that an employee has a limited expectation of privacy in medical information he provided to a physician hired by his employer for the purposes of evaluating the employee’s disability claim); *Urbaniak v. Newton*, 226 Cal.App. 3d 1128 (1991) (holding that a patient’s disclosure of his HIV positive status to a nurse, for the purpose of warning her about the risk of infection, did not amount to

This notion of “limited privacy” does not turn up only in intrusion upon seclusion cases like *Sanders*. Rather, it has found receptive audiences in several other cases involving public disclosure of private facts. Courts willingness to accept “limited privacy” arguments in both the intrusion and public disclosure contexts makes sense, since the intrusion tort’s concept of privacy fully encompasses the conception of privacy that arises in the public disclosure context.⁵² The two leading public disclosure cases appear to be Missouri’s *Y.G. v. Jewish Hospital*,⁵³ and Georgia’s *Multimedia WMAZ, Inc. v. Kubach*,⁵⁴ although a number of other cases contain similar reasoning.⁵⁵

consent for the nurse’s supervising physician to include the patient’s HIV status in a report evaluating the employee’s workers’ compensation claim); *Times Mirror Co. v. Superior Court*, 198 Cal.App.3d 1420 (1988) (holding that the plaintiff had a reasonable expectation of privacy in her having witnessed the murder of her roommate by an at-large suspect, even though she had shared this information with friends, relatives, and police officers).

The only California case that, at first glance, seems like a rejection of “limited privacy” underscores just how far the principle extends. In *Sipple v. Chronicle Publishing Co.*, 154 Cal. App. 3d. 1040 (1984), the California courts held that a plaintiff’s decision to share information about his homosexuality with members of the gay community deprived him of a cause of action when a general circulation San Francisco newspaper mentioned his orientation after he became a public figure by foiling an assassination attempt against President Ford. Sipple argued that his willingness to share his sexual orientation with supportive gays hardly indicated a willingness to share it with unsupportive heterosexuals. Indeed, Sipple’s family shunned him after they learned about his sexual orientation. *Id.* at 1044-45. The court held that Sipple’s sexual orientation had become a matter of public knowledge well before the defendant’s publication, citing the fact that Sipple’s orientation was known to “hundreds of people in a variety of cities, including New York, Dallas, Houston, San Diego, Los Angeles, and San Francisco.” *Id.* at 1047. The court further emphasized that several gay magazines had published stories referencing Sipple’s homosexuality. *Id.* at 1047-48. Against this backdrop, and with Sipple gaining substantial fame by virtue of his heroic act, the court was incredulous that Sipple’s poorly-kept secret would have remained unknown to heterosexuals generally had the defendant not acted. For further discussion of *Sipple*, see *infra* note 207.

⁵² Compare RESTATEMENT (SECOND) OF TORTS § 652(B) (defining intrusion upon seclusion as an intentional intrusion “upon the solitude or seclusion of another or his private affairs or concerns”), with RESTATEMENT (SECOND) OF TORTS § 652(D) (defining public disclosure as giving publicity “to a matter concerning the private life of another”). It is difficult to imagine how something can be another’s “private affair or concern,” but not “a matter concerning the private life of another.”

⁵³ 795 S.W.2d 488 (Mo. Ct. App. 1990).

⁵⁴ 443 S.E.2d 491 (Ga. 1994).

⁵⁵ See, e.g., *Doe v. B.P.S. Guard Serv.*, 945 F.2d 1422 (8th Cir. 1991) (holding that female models who undressed in each other’s presence had a cause of action against peeping Tom security guards, who used a security camera to leer at the models in various states of undress); *Sheets v. Salt Lake County*, 45 F.3d 1383 (10th Cir. 1995) (holding that the plaintiffs’ having turned over a diary to police investigators did not indicate a willingness to have the diary released to an author for use in a published book); *Huskey v. NBC*, 632 F.Supp. 1282 (N.D. Ill. 1986) (holding that a prisoner who worked out in a prison’s exercise cage had a reasonable expectation of privacy against being filmed for a television broadcast, even though other inmates and prison guards could see him exercising); *Vassiliades v. Garfinckel’s, Brooks Bros.*, 492 A.2d 580 (D.C. 1985) (holding that a plaintiff had a privacy claim against those who disclosed that she had undergone plastic surgery, even though the plaintiff had told her family and friends about the procedure); *Benitez v. KFC*, 714 N.E.2d 1002 (Ill. App. Ct. 1999) (holding that male employees’ spying on multiple undressing female employees is intrusion upon seclusion even though the undressed co-workers disrobed in each other’s presence); *Peckham v. Boston Herald*, 719 N.E.2d 888 (Mass. App. 1999) (holding that the plaintiff’s disclosure of his involvement in a paternity suit with his daughter and two close friends did not necessarily waive a reasonable expectation of privacy in that information).

Y.G. involved spouses who found themselves unable to conceive a child naturally. They therefore underwent in vitro fertilization at the defendant hospital, resulting in a pregnancy. Only hospital employees and the mother of one of the plaintiffs knew about the couple's participation in the in vitro program, and the couple apparently did not tell others about their involvement because their church condemned the practice.⁵⁶ Several months into the wife's pregnancy, the couple was invited to a party at the hospital to celebrate the in vitro fertilization program's five-year anniversary.⁵⁷ A camera crew and reporter from a local television station were at the party, and, although the plaintiffs refused to be interviewed and "made every reasonable effort" to avoid being filmed, their image was used on the nightly news, with a voiceover stating that the (unnamed) plaintiffs were expecting triplets as a result of their participation in the program.⁵⁸ After the broadcast, the plaintiffs were chastised by their church and the husband was ridiculed at his workplace.⁵⁹ The defendant argued that the plaintiffs had waived any reasonable expectation of privacy as to their involvement in the in vitro clinic by attending a party that forty other people also attended.⁶⁰ The court rejected this argument, holding that by attending the party the plaintiffs "clearly chose to disclose their participation to only the other in vitro couples. By so attending this limited gathering, they did not waive their right to keep their condition and the process of in vitro private, in respect to the general public."⁶¹

Similarly, in *Multimedia WMAZ v. Kubach*, the plaintiff was an HIV-positive man who had disclosed his condition to relatives, friends, medical personnel, and members of his AIDS support group, approximately sixty people in all.⁶² Kubach agreed to appear on a local television broadcast to discuss AIDS, and was assured by station personnel that his face would be digitized, and hence unrecognizable to the viewing audience.⁶³ The station employee responsible for the digitization evidently set the digitization setting too low, and Kubach was recognized by members of his local community when the broadcast aired.⁶⁴ After Kubach sued the station for invasion of privacy, the station responded by arguing that Kubach had waived his expectation of privacy in his HIV status by disclosing it to his friends, relatives, acquaintances, and medical service providers.⁶⁵ The court disagreed, noting that Kubach had made these disclosures to people who "cared about him . . . or because they also had AIDS."⁶⁶ Although Kubach did not tell his

⁵⁶ 795 S.W.2d at 492-93.

⁵⁷ *Id.* at 492.

⁵⁸ *Id.*

⁵⁹ *Id.* at 493.

⁶⁰ *Id.* at 502; *Id.* at 503, 504 (Gaertner, J., dissenting).

⁶¹ *Id.* at 502.

⁶² 443 S.E.2d at 494 & n.1 (Ga. 1994).

⁶³ *Id.* at 493. The court's opinion makes no mention of Kubach pursuing a cause of action for breach of contract.

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.* at 494.

friends and relatives to keep his HIV status confidential, “there was also testimony that they understood that plaintiff’s condition was not something they would discuss indiscriminately.”⁶⁷

These cases suggest that even if a plaintiff reveals information about himself to dozens of people, and even if there are no legal or contractual constraints on those peoples’ ability to disseminate the information further, the information can remain “private” for the purposes of privacy tort law. Such information can remain private regardless of whether the people to whom the information was initially disclosed were the plaintiffs’ intimates (as in *Kubach*), co-workers (as in *Sanders*), or strangers (as in *Y.G.*).

B. The Hard-Line Cases

Some opinions have rejected a plaintiff’s invocation of limited privacy, holding that his disclosure to a group of persons waived all privacy expectations in the information. New York’s *Nader v. General Motors* has long been a landmark case in privacy law.⁶⁸ The nation’s largest automobile manufacturer tried to discredit and intimidate consumer advocate Ralph Nader prior to the publication of his best seller, *Unsafe at Any Speed*. To that end, General Motors allegedly interviewed Nader’s close friends and business associates about his racial and religious views, his sexual proclivities, his personal habits, and his political beliefs. GM’s agents secured these interviews by falsely telling the interviewees that they worked for a company at which Nader was seeking employment.⁶⁹ Nevertheless, the court rejected Nader’s claim that the interviews amounted to an intrusion upon Nader’s seclusion or private affairs.⁷⁰

Although those inquiries may have uncovered information of a personal nature, it is difficult to see how they may be said to have invaded the plaintiff’s privacy. Information about the plaintiff which was already known to others could hardly be regarded as private to the plaintiff. Presumably, the plaintiff had previously revealed the information to such other persons, and he would necessarily assume the risk that a friend or acquaintance in whom he had confided might breach the confidence.⁷¹

The court thus found unpersuasive the argument that Nader’s disclosure to this network of close friends and associates maintained the privacy of the information that he had shared. Indeed, the court rejected a basic premise of limited privacy – the idea that one’s associates may be willing to share confidential information with people who were considering employing Nader, but not with a corporation that was trying to discredit

⁶⁷ *Id.*

⁶⁸ 255 N.E.2d 765 (N.Y. 1970).

⁶⁹ *Id.* at 564.

⁷⁰ Because GM never publicly disclosed the dirt that it may have dug up on Nader, he sued for intrusion upon seclusion rather than public disclosure of private facts.

⁷¹ *Id.* at 568-69.

him.⁷² According to the court, once one shares a fact about himself with a friend, that fact is no longer private, as a matter of law.

A Michigan case provides further illumination. Consuelo Sanchez Duran was a Columbian judge who had indicted the notorious drug lord, Pablo Escobar.⁷³ After she and her family received several death threats, she resigned from the bench and fled the country. Duran took a job as the Columbian Consul in Detroit, and signed a lease for an apartment in the area.⁷⁴ The State Department hired security guards to protect Duran. Duran used her real name when shopping in stores or eating at restaurants and told a few of her curious neighbors that she had been threatened by drug dealers.⁷⁵ At the same time, Duran “kept an unlisted telephone number, did not join any social clubs or organizations, and did not attend any concerts, sporting events, or motion pictures.”⁷⁶ A few months after Duran moved to Detroit, local reporters exposed Duran’s history and disclosed her address, providing readers and television viewers with photographs of her apartment complex.⁷⁷ At least one reporter also described a \$1 million bounty that the Columbian drug cartel had placed on Duran’s head.⁷⁸ Duran sued the media outlets for public disclosure of private facts, but the courts affirmed the lower courts’ decision to grant the defendants summary judgment. In the court’s assessment, the plaintiff’s actions in the United States had rendered her identity “open to the public eye.”⁷⁹

⁷² Alabama has followed *Nader*’s approach in two recent opinions. See *Myrick v. Barron*, 820 So.2d 81, 85 (Ala. 2001) (“Barron’s argument fails, however, because interviews of other people about their knowledge of Barron could reveal only information already known (or allegedly known) by those people. . . . Can information which other people claim to know about Barron be protected as ‘private’ and, thereby, be shielded from inquiry by this branch of the invasion-of-privacy tort? Common sense and legal precedent dictate a negative response to this question.”); *Johnston v. Fuller*, 706 So.2d 700, 702-03 (Ala. 1997) (“Johnston’s allegations concern only voluntary interviews in which the defendants learned information already known to others. This information is not protected by the limited scope of the wrongful-intrusion branch of the invasion of privacy tort.”).

The Ninth Circuit has held that Arizona courts would also reject California’s expansive application of the doctrine of “limited privacy.” See *Medical Lab. Mgmt. Consultants v. ABC*, 306 F.3d 806, 815 (9th Cir. 2002) (“The question before us then is whether Arizona law would recognize as objectively reasonable Devaraj’s subjective expectation that his conversation with the ABC representatives would not be broadly disseminated to others . . . [W]e conclude that, under Arizona law, Devaraj could not have reasonably expected privacy against the ABC representatives’ secret videotaping of his communications with them. We conclude that the Arizona Supreme court would not recognize as broad an interest in limited privacy as the California Supreme Court has done.”).

⁷³ *Duran v. Detroit News, Inc.*, 504 N.W.2d 715 (Mich. Ct. App. 1993).

⁷⁴ *Id.* at 718.

⁷⁵ *Id.*

⁷⁶ *Id.*

⁷⁷ *Id.*

⁷⁸ *Id.* at 721.

⁷⁹ *Id.* at 72; see also *Stressman v. American Black Hawk Broadcasting Co.*, 416 N.W.2d 685, 687 (Iowa 1987) (holding that, as a matter of law, a plaintiff would have no reasonable expectation of privacy against being filmed while eating in an ordinary restaurant, but might have such an expectation if seated in a restaurant’s private dining room).

Fisher v. Ohio Department of Rehabilitation and Correction,⁸⁰ completes the trilogy of interesting hard-line opinions. In that case, the plaintiff told three co-workers that some of her interactions with her seven-year-old son had “sexual overtones.” The court held that this disclosure rendered the information non-private, such that the plaintiff’s employer was free to disclose the information to her soon-to-be ex-husband.⁸¹ In the court’s view “the report merely recounts a conversation which the plaintiff *publicly and openly* conducted with her fellow employees. The plaintiff’s discussion of her personal experiences were freely offered to the persons around her without concern of the impact it might have on her character.”⁸²

By way of summary, then, what constitutes a “private” matter for the purposes of privacy tort law is not obvious. The courts are not being terribly explicit or precise about why particular disclosures waive privacy expectations and others do not. Certainly, a simple head-counting approach does not reconcile the precedents. After all, Kubach’s disclosure of facts to sixty people did not render them public, but Fisher’s disclosure to three people did.

⁸⁰ 578 N.E.2d 901 (Ohio Ct. Cl. 1988).

⁸¹ Fisher’s disclosures were not communicated to a large audience, at least not until she filed her lawsuit. Although some jurisdictions, such as Illinois, treat the public disclosure tort’s “publicity” element as having been satisfied by a disclosure to a small group of people with whom the subject has a special relationship, Ohio rejects this approach. *Compare* *Miller v. Motorola*, 560 N.E.2d 900 (Ill. App. 1990), *with Fisher*, 578 N.E.2d at 903. The *Fisher* court identified the lack of publicity as an additional reason for dismissing Fisher’s privacy claim. In my view, *Fisher*’s conception of publicity is far more appealing than *Miller*’s. The *Miller* standard will render some casual gossip by unsophisticated parties actionable. By making the relevant social network for privacy law purposes a handful of people, Illinois law has the potential to deter a great deal of socially valuable communication. *See also* RESTATEMENT (SECOND) OF TORTS § 652D, comment b (siding with the Ohio view of publicity).

⁸² *Id.* at 903 (emphasis added).

Another line of privacy authority is broadly consistent with the *Nader / Fisher / Duran* approach to limited privacy. This line of cases suggests that a subject does not have a reasonable expectation of privacy with respect to acts that occur in public places or are otherwise visible to the public. *See* DANIEL J. SOLOVE & MARC ROTENBERG, *INFORMATION PRIVACY LAW* 95-96 (2003) (collecting cases); Lance E. Rothenberg, Comment, *Re-thinking Privacy: Peeping Toms, Video Voyeurs, and the Failure of Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space*, 49 AM. U. L. REV. 1127, 1146-55 (2000) (same); *but see* *Daily Times Democrat v. Graham*, 162 So.2d 474 (Ala. 1964) (permitting a tort suit by a woman who was photographed at a county fair with her skirt blown up over her head, relying in part on the fact that the photographer was lying in wait to catch the woman in an embarrassing situation); *Cook v. WHDH-TV, Inc.*, 37 Media L. Rep. 1242, 1999 WL 1327222, at *5 (Mass. Super. Mar. 4, 1999) (noting that “[c]auses of action for intrusions on one’s right to privacy . . . are ordinarily foreclosed when the invasion occurs in a public place. This is so because the plaintiff is said to have voluntarily assumed the risk of being observed by being in a public place.”; and holding, nevertheless, that the plaintiff could withstand summary judgment after being filmed with his son in a parked car at a Burger King parking lot). Hence, a couple photographed kissing at a farmer’s market has no cause of action against a news magazine that published this photograph, *Gill v. Hearst Pub. Co.*, 253 P.2d 441, 444-45 (Cal. 1953), a couple filmed walking from their home to a squad car has no expectation of privacy in such footage, *Reeves v. Fox Tele. Network*, 983 F. Supp. 703, 709 (N.D. Ohio 1997), and a high school athlete whose genitalia were exposed in a soccer match photograph that was published in a newspaper had no privacy cause of action, *McNamara v. Freedom Newspapers, Inc.*, 802 S.W.2d 901, 905 (Tex. Ct. App. 1991). If a tree falls in a public forest, the images of its fall become public, even if the photographer who captures it on film was the only person around to see it fall.

All these cases involve judicial efforts to assess the flow of information through social networks. At this point, it therefore seems appropriate to examine how a sociologist might try to answer the questions that courts are considering in these kinds of cases.

III. Social Network Theory

For the past several decades, sociologists, epidemiologists, computer scientists, electrical engineers, economists, and researchers from various other fields have been converging on an understanding of the way that much of the world works, best described as “network theory.”⁸³ The basic challenge of network theory is to understand how change occurs and is transmitted among adjacent units in any kind of network.⁸⁴ Perhaps surprisingly, the same basic insights about network structure have been found applicable to a variety of disparate disciplines. For example, scholars studying the flow of electricity through power grids have noticed substantial structural similarities to the way that impulses make their way through the neural networks of various species.⁸⁵ Similarly, epidemiologists are examining how diseases spread through particular populations, looking at the levels of connectedness between members of an at-risk population,⁸⁶ in much the same way that scholars of organizational structure have studied the overlapping memberships of American corporate boards of directors, searching for clues about the

⁸³ For accessible, cross-disciplinary analyses of network theory, see DUNCAN WATTS, *SIX DEGREES: THE SCIENCE OF A CONNECTED AGE* (2003), and ALBERT LASZLO BARABASI, *LINKED: HOW EVERYTHING IS CONNECTED TO EVERYTHING ELSE AND WHAT IT MEANS FOR BUSINESS, SCIENCE, AND EVERYDAY LIFE* (2003).

Just one month after my paper appeared on SSRN, Thomas Smith posted a very interesting working paper, in which he notes that federal case law is itself a scale-free network, with certain precedents functioning as hubs and most functioning as obscure nodes. See Thomas A. Smith, *The Web of Law* (January 3, 2005), available in <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=642863>. Smith’s paper makes several fascinating observations about the implications of this finding for the development of legal precedent more generally. For an earlier application of a few aspects of network theory to international law, see Kal Raustiala, *The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law*, 43 VA. J. OF INT’L L. 1 (2002); see also Amitai Aviram, *Regulation by Networks*, 2003 B.Y.U. L. REV. 1139, 1223-37 (discussing network structure more generally).

⁸⁴ Network theorists tend to focus on network structure and relationships as a means of understanding social phenomena. See Timothy J. Rowley, *Moving Beyond Dyadic Ties: A Network Theory of Stakeholder Influences*, 22 ACADEMY OF MGMT. REV. 887, 897 (1997).

⁸⁵ Duncan J. Watts, *Networks, Dynamics, and the Small-World Phenomenon*, 105 AM. J. OF SOCIOLOGY 493, 515-16 (1999).

⁸⁶ See, e.g., David C. Bell et al., *Centrality Measures for Disease Transmission Networks*, 21 SOCIAL NETWORKS 1 (1999); Fredrik Lijeros et al., *The Web of Human Sexual Contacts: Promiscuous Individuals Are the Vulnerable Nodes to Target in Safe-Sex Campaigns*, 907 NATURE 411, 411-12 (2001) (“Our results may have epidemiological implications, as epidemics arise and propagate much faster in scale-free networks than in single-scale networks. Also, the measures adopted to contain or stop the propagation of diseases in a network need to be radically different for scale-free networks. Single-scale networks are not susceptible to attack at even the most connected nodes, whereas scale-free networks are resilient to random failure but are highly susceptible to destruction of the best-connected nodes.”).

effects of inter-connectedness on corporate governance.⁸⁷ Whether scientists are discussing computer networks, social networks,⁸⁸ or biological networks, the same “scale-free” patterns of network structure are frequently observable.⁸⁹

A scale-free network, sometimes called a “power-law” network, has a very large number of poorly connected nodes (called “peripherals”) and a smaller number of highly connected nodes (called “supernodes” or “hubs”) that actively transmit lots of data to many other nodes.⁹⁰ We can contrast this scale-free structure with a random network structure, where one would expect each node in a network to have approximately the same number of links to other nodes. This distinction becomes relevant for our purposes because it turns out that most human social networks, particularly information networks, are scale-free.⁹¹

Figure 1 contrasts a “pure” scale-free structure on the left, with a random structure on the right. In the pure scale-free network each (relatively isolated) peripheral actor (P) is connected to a single (well-connected) supernode (S).⁹² There are a total of eight links in the scale-free network, each represented by a line. In the random network, there are also a total of eight links among actors, and each actor is connected to between one and three other actors. Even a cursory examination of the diagrams below shows that a scale-free structure is far more efficient at linking up a society of actors, provided, of course, that all connections and actors are stable, and that there is no danger of network congestion. For example, P1 and P3 can be connected via two links in the scale-free network, as can any other peripherals. In the random network, however, connecting actors presents much greater difficulties. Linking up P1 and P3 requires connecting via

⁸⁷ See, e.g., Gerald F. Davis, Mina Yoo & Wayne E. Baker, *The Small World of the American Corporate Elite, 1982-2001*, 1 STRATEGIC ORGANIZATION 301, 321-322 (2003) (“On average any two of the 4538 directors of the 516 largest US firms . . . in 1999 could be connected by 4.3 links, and any two of the boards are 3.5 degrees distant. Mills saw a small set of private schools, such as Groton and Exeter, providing an essential agency for socializing and organizing members of the upper class, and Mintz and Schwartz argued for a special role for money-centered banks in knitting together corporate directors. But our results suggest that the small-world organization of the corporate elite is an emergent property of networks *qua* networks and requires no coordinating mechanism whatsoever, for the same reasons that brains, power grids, and the World Wide Web are also small worlds.”).

⁸⁸ In the social context, a “network consists of a set of individuals and of the links among them. Links between pairs of individuals might represent a wide range of connections, including such activities as friendship, advice seeking, informational communication, and material transfers.” David Krackhardt & Robert N. Stern, *Informal Networks and Organizational Crises: An Experimental Simulation*, 51 SOCIAL PSYCH. Q. 123, 127 (1988).

⁸⁹ WATTS, *supra* note 83, at 107; Lada A. Adamic & Eytan Adar, *Friends and Neighbors on the Web*, 25 SOCIAL NETWORKS 211, 215 (2003).

⁹⁰ WATTS, *supra* note 83, at 107.

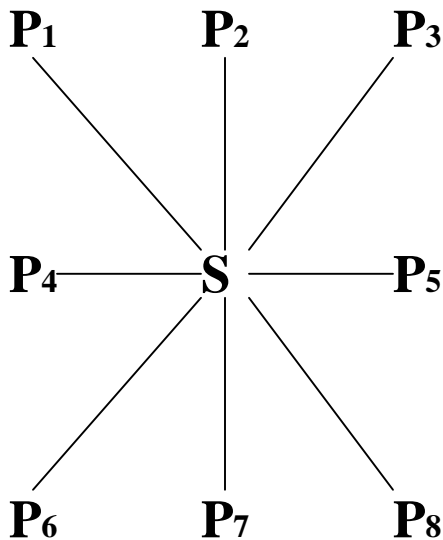
⁹¹ Adamic & Adar, *supra* note 89, at 215; Daniele Bondonio, *Predictors of Accuracy in Perceiving Informal Social Networks*, 20 SOCIAL NETWORKS 301, 306 (1998); Ronald S. Burt, *Structural Holes and Good Ideas*, 110 AM. J. SOCIOLOGY (forthcoming 2004) (manuscript at 3); A. Kimball Romney & Katherine Faust, *Predicting the Structure of a Communications Network from Recalled Data*, 4 SOCIAL NETWORKS 285, 296 (1982); Rebecca W. Tardy & Claudia L. Hale, *Getting “Plugged in”: A Network Analysis of Health-Information Seeking Among ‘Stay-at-Home Moms,’* 65 COMMUNICATION MONOGRAPHS 336, 352-53 & tbl. 3 (1998).

⁹² For an explanation of this terminology, see *infra* text accompanying notes 99-100.

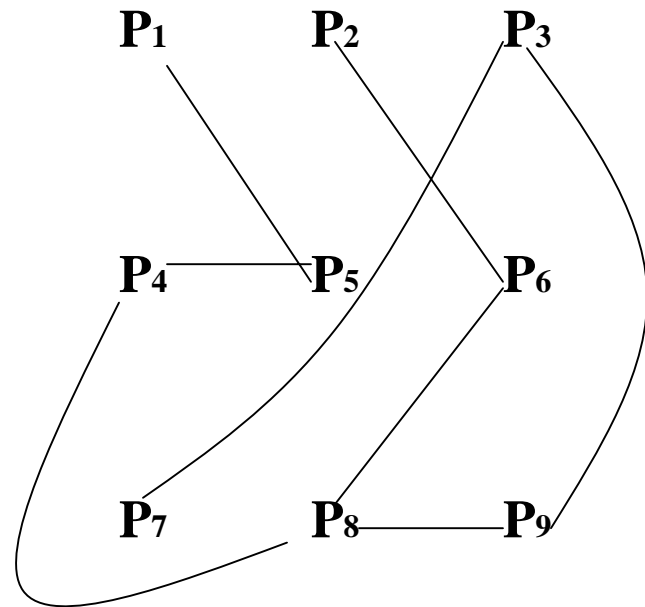
P5, P4, P8, and P9. Indeed, with only eight connections and nine actors, there is a substantial possibility that the members of a random network will not be able to connect at all. So if one removes the linkage between P4 and P5, and replaces it with a linkage connecting P7 and P6, at least two of the actors (P1 and P5) will become entirely isolated from the group.

Figure 1: Scale-Free Networks versus Random Networks

“Pure” Scale-Free Network



Random Network



In the context of social connections, the scale-free social structure can be illustrated using the only social networking game that has penetrated American popular culture: Six Degrees of Kevin Bacon. In 1997, fraternity brothers at William and Mary discovered that the actor Kevin Bacon could be connected to virtually all of the roughly half a million people who had acted in feature films since 1898.⁹³ The students popularized a game, the object of which was to figure out how to connect a particular actor to Kevin Bacon in the fewest number of links possible. For instance, the actor Laurence Fishburne appeared in *Mystic River* with Kevin Bacon in 2003. Fishburne is one of 1,673 actors with a Bacon number of one. Carrie-Anne Moss has not appeared in a film with Kevin Bacon, but co-starred in the *Matrix* films with Laurence Fishburne, so she has a Bacon number of two, along with 130,850 other actors. Justin Allder, is one of 349,031 actors who has a Bacon number of three, having appeared in the obscure 1996

⁹³ BARABASI, *supra* note 83, at 93-96; *see also* The Oracle of Bacon at Virginia, available at <http://www.cs.virginia.edu/oracle/> (visited May 9, 2004) (noting that 12% of the movie actor universe cannot be linked to the rest of the movie universe, either because they appeared in straight-to-video films not included in the Internet Movie Database, or because they have not appeared in any films with mainstream Hollywood actors).

film, *Sabotage*, with Carrie-Anne Moss, who appeared in the *Matrix* films with Laurence Fishburne, who appeared in *Mystic River* with Kevin Bacon.⁹⁴

The average actor in the Internet Movie Database has a Kevin Bacon number of 2.941 – meaning that he can be connected to Kevin Bacon through less than two other actors. This means Bacon is quite well connected to Hollywood actors, but there are actually 1,221 actors in the Internet Movie Database who are even better connected than Kevin Bacon.⁹⁵ Rod Steiger – yes, Rod Steiger⁹⁶ – was evidently the best connected Hollywood Actor of all time, with the average Internet Movie Database actor having a Rod Steiger number of 2.676 as of April 2003.⁹⁷

This data from the Internet movie database helps us understand the way in which human social networks work. There are hundreds of thousands of obscure actors in the Internet Movie Database, such as Deborah Reagan, who appeared in only two films during her career. She happens to have a Kevin Bacon number of one, because she played Kevin Bacon's wife in the 1979 film, *Starting Over*. (Bacon and Reagan had bit parts in that movie.) In any event, we can contrast the plethora of Deborah Reagans with the few thousand Kevin Bacons and Rod Steigers who connect everyone in the actor's guild to everyone else.⁹⁸ Reagan has a Bacon number of one, but her presence in the Internet Movie Database isn't facilitating anyone else's connections. She's just taking up space at the periphery.

As we imagine our own lives and our own social networks, we can all identify some Kevin Bacons and lots of Deborah Reagans.⁹⁹ There are people who stay in touch with old friends, throw dinner parties, play matchmaker, and, most importantly, have close friends in a variety of different cliques. These are the Kevin Bacons of the world:

⁹⁴ See *Who is the Center of the Hollywood Universe*, available at <http://oracleofbacon.org/oracle/center.html> (visited May 9, 2004) (noting that as of April 2003, 1673 actors had a Bacon number of one; 130,851 actors had a Bacon number of two; 349,031 had a Bacon number of three; 84,165 had a Bacon number of four; 6718 had Bacon numbers of five; 788 actors had a Bacon number of six; 107 actors had Bacon numbers of seven; and eleven known actors had a Bacon number of eight).

⁹⁵ *Id.*

⁹⁶ Steiger is best known for playing Charley in *On the Waterfront*, where he acted opposite Marlon Brando in the famous "I could've been a contender" scene. Steiger won the Best Actor Academy Award for the 1967 film, *In the Heat of the Night*.

⁹⁷ The remainder of the top ten list consists of Christopher Lee, Dennis Hopper, Donald Pleasence (who?), Donald Sutherland, Max Von Sydow, Anthony Quinn, Charlton Heston, Harvey Keitel, and Martin Sheen. Shelley Winters is the most connected actress – she ranks twenty-first all time. See http://oracleofbacon.org/oracle/center_list.html (visited May 9, 2004).

⁹⁸ One variation on the Kevin Bacon game involves non-actors. Ordinary citizens can compare how many degrees of separation they are from Kevin Bacon, using personal connections instead of acting roles. This version of the Kevin Bacon game recently was made the subject of a successful Visa television commercial. See Kevin Bacon Central, *Six Degrees of Kevin Bacon*, available in <http://www.allstarz.org/kevinbacon/six.htm#> (visited June 7, 2004).

⁹⁹ This is particularly true once we exclude kin from people's social network. Kin relationships are less voluntary than other kinds of relationships, and most people maintain at least some connections to their families. Kin thus play a role in promoting the equalization of social network size among introverts and extroverts. See Henry W. Irving, *Social Networks in the Modern City*, 55 SOCIAL FORCES 867, 868 (1977).

society's supernodes.¹⁰⁰ The Deborah Reagans of the world, by contrast, are more isolated, hermitted, and aren't introducing people who wouldn't otherwise meet each other. Deborah Reagan may have some friends, but her friends all know one another already, so she's not facilitating new connections. She is a classic peripheral.

A real social network, of course, is more complicated than the Kevin Bacon actors' network. Most pertinently, a real social network is dynamic, not static.¹⁰¹ People are constantly making new connections *and* old connections are disappearing, through death, quarrels, geographic constraints, or simple indifference.¹⁰² Each of us can recall friends from elementary school, high school, or college, with whom we've lost touch, along with scores of former neighbors, co-workers, service providers, and acquaintances. In the Kevin Bacon world, by contrast, Rod Steiger continues to promote network connectedness even though he died two years ago. Still, the similarities between an actors' network and a normal social network are substantial. While communications networks among humans generally are not "pure" scale-free networks like the one pictured in Figure 1, they do exhibit a strong tendency toward scale-free structure, with substantial clustering among members, and a minority of supernodes who facilitate the interactions between members who would not otherwise meet.¹⁰³ Moreover, ties among members of well-connected social clusters can be expected to become stronger as time passes: The more time I spend socializing with Joe, the higher the odds become that I will be introduced to one of Joe's other good friends.¹⁰⁴

All that said, what's interesting about the Kevin Bacon network is precisely what's interesting about human societies in general. A rural farmer in Omaha and a banker in Boston may be separated by only a few links, and yet they will live their entire lives oblivious to each other's existence.¹⁰⁵ When exponential functions like these operate, humans are sometimes genuinely surprised. Two strangers seated next to each other on an airplane might utter with great sincerity the clichéd observation that "it's a small world" upon realizing that they both know someone in common who resides in a

¹⁰⁰ Herminia Ibarra & Steven B. Andrews, *Power, Social Influence, and Sense Making: Effects of Network Centrality and Proximity on Employee Perceptions*, 38 ADMIN. SCI. Q. 277, 279 (1993). For a typology of different types of supernodes, see KIMMEL, *supra* note 19, at 101.

As used in this paper, having many friends and acquaintances does not suffice to make an individual a supernode. Rather, the supernode has many friends and acquaintances who are not independently connected *and* actively shares information with many of those far-flung friends and acquaintances. Thus, someone who has many friends but is very discrete may well be an ordinary node, whereas someone who is constantly sharing new information with a smaller number of friends could be a supernode.

¹⁰¹ For a paper exploring some of the differences in static and dynamic social network models, see Vincent Buskens & Kazuo Yamaguichi, *A New Model for Information Diffusion in Heterogeneous Social Networks*, 29 SOCIOLOGICAL METHODOLOGY 281 (1999).

¹⁰² Ronald S. Burt, *Bridge Decay*, 24 SOCIAL NETWORKS 333 (2002); Karen Klein Inkkink & Theo Van Tilburg, *Broken Ties: Reciprocity and Other Factors Affecting the Termination of Older Adults' Relationships*, 21 SOCIAL NETWORKS 131 (1999).

¹⁰³ See *supra* note 91.

¹⁰⁴ Scott L. Feld, *The Focused Organization of Social Ties*, 86 AM. J. OF SOCIOLOGY 1015, 1019-20 (1981).

¹⁰⁵ Jeffrey Travers & Stanley Milgram, *An Experimental Study of the Small World Problem*, 32 SOCIOMETRY 425 (1969).

distant city. The danger, however, is not this occasional surprise. The danger, at least from a privacy perspective, is that people learn to stop being surprised by these encounters, and guard their personal information too much as a consequence.¹⁰⁶ Even though our farmer and banker might be connected through only a few links, it will be exceedingly rare for one of them to hear a story about the other. When only a few or no links connect a group of Boston bankers and Omaha farmers, they are separated by what Ronald Burt calls a “structural hole,” a lack of effective ties between the groups that renders the probability of information exchange quite low, even if both parties could benefit substantially from such communication.¹⁰⁷

This point is critical to the study of how previously private information spreads through society. In scale-free social networks, there is always *the potential* that information any person discloses to any other person will spread to the entire world.¹⁰⁸ By some fluke, any bit of information might be widely distributed. Yet, as I will argue below, in light of the prevalence of structural holes between certain social networks, people will be well-served by ignoring this possibility, and the law ought to validate their decision to do so. Relatedly, whether information becomes “public” will depend on whether it reaches a supernode or not, and whether the supernode finds the information worth disseminating. As I will suggest in Part IV, the fact that information has reached one defendant supernode hardly renders it inevitable that it would have reached another supernode in the defendant’s absence.

A. *The Strength of Weak Ties*

There are people with whom we frequently exchange information about a number of different topics, and people with whom we share less information, about a narrower range of topics. Sociologists generally refer to relationships falling into the former category as “strong ties” or “high intensity” and relationships falling into the latter category as “weak ties” or “low intensity.”¹⁰⁹ Assume I have two neighbors. Neighbor A and I frequently discuss work, sports, television, romantic involvements, and politics. Neighbor B and I occasionally discuss the weather and exchange pleasantries. My relationship with A is a strong tie. My relationship with B is a weak tie.

In the real world, we can map these relationships onto organizational structures. Imagine a large law firm in a big city. As a general matter, attorneys within the tax

¹⁰⁶ Indeed, some social networks research suggests a tendency for this to occur. See Eric Kumbasar et al., *Systematic Biases in Social Perception*, 100 AM. J. OF SOCIOLOGY 477, 498 (1994) (finding that people systematically overestimate the extent to which their friends communicate with each other).

¹⁰⁷ RONALD S. BURT, *STRUCTURAL HOLES* (1992).

¹⁰⁸ This is true of all information. A joke I tell one other person could conceivably spread to the entire United States population. And yet, to the best of my knowledge, that’s never occurred. Perhaps if my jokes were funnier . . .

¹⁰⁹ JOHN SCOTT, *SOCIAL NETWORK ANALYSIS* 32 (2d ed. 2000); Gabriel Weimann, *The Strength of Weak Conversational Ties in the Flow of Information and Influence*, 5 SOCIAL NETWORKS 245, 246 (1983); see also Daniel J. Brass et al., *Relationships and Unethical Behavior: A Social Network Perspective*, 23 ACADEMY OF MGMT. REV. 14, 17 (1998) (“The strength of a relationship refers to the frequency, reciprocity, emotional intensity, and intimacy of that relationship. Casual acquaintances, represented by infrequent interaction and indifferent affect, are characterized by weak ties.”).

department will have relatively strong ties to other attorneys in the same firm's tax department, and weaker ties to attorneys in the firm's intellectual property litigation department.¹¹⁰ There will be some strong ties that cross departmental lines – for example, the attorneys who serve on the firm's hiring committee or management committee are likely to spend a great deal of time talking to each other. But as a general matter, intra-department ties will be stronger and inter-department ties will be weaker.

As one moves outside the firm, the same patterns hold. A tax attorney at Jenner & Block in Chicago may have strong ties to a tax attorney at Kirkland & Ellis in Chicago, based on having worked on deals together in the past or simultaneous service on bar association committees. But most professional ties outside of one's own law firm will be weak ties, and in a large city like Chicago, the vast majority of lawyers will not know each other personally.¹¹¹ That said, the social distance between an intellectual property litigator at Kirkland & Ellis and a tax attorney at Jenner & Block will not be substantial. There is probably at least one person who knows both lawyers, and so an introduction between the two attorneys could be arranged rather easily.¹¹²

Mark Granovetter's work on "the strength of weak ties" has become a canonical text in the study of social networks.¹¹³ Granovetter observed that social networks tend to be highly clustered: I have very close ties to people in my family, but they have close ties to each other, too, and their connectedness is not dependent on me.¹¹⁴ People within a closely-knit network are likely to be quite similar to one another – they may share the same jobs, neighborhoods, last names, knowledge base, or alumni connections.¹¹⁵ As a result, relationships within a close-knit group have high levels of transitivity¹¹⁶ – all of my friends on my law school's faculty are friends with each other as well. This makes information redundant within a network of people bound together by strong ties. By the time I learn new and interesting information from a colleague, it is likely that other

¹¹⁰ Cf. Morten T. Hansen, *The Search-Transfer Problem: the Role of Weak Ties in Sharing Knowledge Across Organization Subunits*, 44 ADMIN. SCI. Q. 82, 106 (1999) (discussing a similar phenomenon among engineers).

¹¹¹ John P. Heinz et al., *The Constituencies of Elite Urban Lawyers*, 31 LAW & SOCIETY REV. 441 (1997) (noting that even highly prominent members of Chicago's legal community were not directly tied to most lawyers surveyed).

¹¹² Indeed, directed networking seems to occur within large law firms with some regularity. When I worked at a large Seattle law firm, someone would occasionally send out an email to all the lawyers at the firm asking if anyone knew Mr. So-and-So. Mr. So-and-So was usually a potential client, mediator, or co-counsel. Another effective strategy would be to obtain the Martindale Hubbell biography of the target, and then search for people within one's own firm who share a possible tie. Most obviously, one might look for someone who graduated from the same law school at roughly the same time.

¹¹³ Mark Granovetter, *The Strength of Weak Ties: A Network Theory Revisited*, 1 SOCIOLOGICAL THEORY 201 (1983).

¹¹⁴ *Id.* at 201-02. Other studies of social networks have found substantial clustering of social ties within racial and ethnic groups. See Charles Korte & Stanley Milgram, *Acquaintance Networks Between Racial Groups: Application of the Small World Method*, 15 J. OF PERSONALITY & SOCIAL PSYCH. 101, 107 (1970); Gabriel Wiemann, *The Not-So-Small World: Ethnicity and Acquaintance Networks in Israel*, 5 SOCIAL NETWORKS 289, 297 (1983).

¹¹⁵ Granovetter, *supra* note 113, at 204.

¹¹⁶ *Id.* at 218; Wiemann, *supra* note 109, at 260-63.

colleagues with whom I am strongly tied would have already learned it, or will learn it soon enough even if I do not tell them.

Strong ties are plainly a source of strength, but relying exclusively on close ties for sources of information is a bad idea. As Granovetter argues: “Individuals with few weak ties will be deprived of information from distant parts of the social system and will be confined to the provincial news and views of their close friends.”¹¹⁷ Granovetter suggests that the economically disadvantaged tend to rely too much on strong ties.¹¹⁸ And because strong ties are so much costlier to maintain than weak ties,¹¹⁹ poor people’s heavy investments in strong ties preclude them from developing valuable weak ties.

Granovetter’s research suggests that weak ties are often critical in helping individuals learn about new job opportunities.¹²⁰ Weak ties serve a “bridging” function, transferring new information from one closely-knit group to another.¹²¹ Information gained from weak ties is therefore more likely to be new and non-redundant. Granovetter found that weak ties were particularly instrumental in helping managers and professionals find jobs.¹²² Notably, each individual weak tie has a low probability of transferring useful information, but because so many weak ties exist, their sheer numbers make them, in the aggregate, a critical source of new and valuable information.¹²³ Strong ties could be useful too, particularly in job-seeking contexts where an unemployed person needed help from a social contact who was highly motivated to help him find work.¹²⁴

Granovetter’s analysis of how information about job openings gets transmitted through a social network has obvious applications to the study of information diffusion

¹¹⁷ *Id.* at 202.

¹¹⁸ *Id.* at 213; see also Matthijs Kalmijn, *Shared Friendship Networks and the Life Course: An Analysis of Survey Data on Married and Cohabiting Couples*, 25 *SOCIAL NETWORKS* 231 (2003) (finding that well-educated people have more friends, but spend less time with them, than their lesser-educated counterparts); Brian R. Patterson, *Communication Network Activity: Network Attributes of the Young and Elderly*, 42 *COMMUNICATION Q.* 155 (1995) (finding that the elderly tend to rely more on strong ties, and less on weak ties, as they age).

¹¹⁹ Hansen, *supra* note 110, at 105; Giuseppe Labianca, Daniel J. Brass, & Barbara Gray, *Social Networks and Perceptions of Intergroup Conflict: The Role of Negative Relationships and Third Parties*, 41 *ACADEMY OF MGMT. J.* 55, 58 (1998). See generally Krackhardt & Stern, *supra* note 88, at 127-28 (“[I]ndividuals have a limited amount of time, energy, and need for the social interaction and intimacy which are demanded in maintaining friendships. Given this assumption, one will find, on the average, a tradeoff between the number of friends one can maintain outside the subunit and the number one can maintain inside the subunit.”).

¹²⁰ Granovetter, *supra* note 113, at 205.

¹²¹ Weimann, *supra* note 109, at 254-56, 264. In another study, Wiemann examined the ability of Ashkenazi and Sephardic Jews in Israel to reach target individuals through chains of social connections. He found substantial segregation of social networks along ethnic lines, and determined that efforts to contact a target individual often failed because of a lack of contacts between Ashkenazi and Sephardic Jews. Wiemann, *supra* note 114, at 298.

¹²² Granovetter, *supra* note 113, at 208.

¹²³ Noah E. Friedkin, *Information Flow Through Strong and Weak Ties in Intraorganizational Social Networks*, 3 *SOCIAL NETWORKS* 273, 284-85 (1982).

¹²⁴ Granovetter, *supra* note 113, at 209.

generally. Information dissemination through the wider society often depends on weak ties:

What makes cultural diffusion possible, then, is the fact that small cohesive groups who are liable to share a culture are not so cohesive that they are entirely closed; rather, ideas may penetrate from other such groups via the connecting medium of weak ties. It is a seeming paradox that the effect of weak ties, in this case, is homogenization, since my emphasis has been the ability of weak ties to reach out to groups with ideas and information different from one's own. The paradox dissolves, however, when the process is understood to occur over a period of time. The ideas that initially flow from another setting are, given regional and other variations, probably new. Homogenous subcultures do not happen instantly, but are the *endpoint* of diffusion processes.¹²⁵

In Granovetter's framework, weak ties help explain the spread of everything from knowledge to fads from one edge of the global social network to the other. Follow-up work by other sociologists has revealed that weak ties are particularly important in spreading gossip and news, but information about new products and consumer opportunities is generally spread through stronger ties.¹²⁶ The chief advantage of information diffusion through weak ties stems from the rapidity with which information is transmitted between different close-knit groups.¹²⁷ Information transmitted via strong ties generally spreads less quickly, but is more accurate and credible.¹²⁸

Those who actively spread information via many weak ties function as supernodes, and are likely to gain economic and status advantages because they are the first members of their close-knit groups to learn about new information that has originated in far-flung, close-knit groups.¹²⁹ These supernodes tend to be happier and better informed than the peripherals.¹³⁰ Supernodes are more likely to be perceived as

¹²⁵ *Id.* at 215-16.

¹²⁶ Weimann, *supra* note 109, at 254-55.

¹²⁷ *Id.* at 258.

¹²⁸ *Id.*

¹²⁹ See Gordon W. Allport & Leo Postman, *An Analysis of Rumor*, 10 PUB. OPINION Q. 501, 512 (1946-47) (discussing the prestige associated with being the first to share truthful, newsworthy information with a group); While supernodes tend to be the highest-status individuals in a social network, there may be costs associated with supernode status in certain contexts. For example, Wayne Baker and Robert Faulkner found that central players in price-fixing conspiracies faced a greater risk of prosecution and longer sentences than peripheral members of such conspiracies. Wayne E. Baker & Robert R. Faulkner, *The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry*, 58 AM. SOCIOLOGICAL REV. 837, 854 (1993). Baker and Faulkner suggest that there are more possible witnesses who can cooperate with government prosecutors and testify against a supernode. Because a more peripheral member has fewer contacts within the conspiracy, there are fewer people who could testify against him. *Id.* at 855 n. 14. This seems plausible, but I also suspect that prosecutors view the supernodes of criminal conspiracies as more culpable than the peripheral members, so they may seek harsher sentences against these individuals. For another discussion of gossip and information flow issue unique to the organized crime setting, see Gambetta, *supra* note 19, at 220-22.

¹³⁰ Ronald S. Burt, *The Social Capital of Opinion Leaders*, 567 ANNALS OF AMER. ACADEMY OF POLITICAL & SOC. SCI. 37, 50 (2000) (finding that supernodes "enjoy more positive job evaluations, faster promotions,

“leaders” and are more likely to earn promotions within a workplace.¹³¹ Supernodes maintain their privileged status by continuing to serve as information clearinghouses, and, in certain contexts, become supernodes based in part on their willingness to share previously private information about themselves.¹³²

That said, there will be certain types of information that do not lend themselves to communication via weak ties. For example, scholars studying product innovation have suggested that weak ties function quite well at facilitating searches for stand-alone information, but are not particularly successful means of transferring complex knowledge.¹³³ This suggests an aggregation difficulty – if two different people have two pieces of information that must be aggregated to yield a useful result, it is more likely that they will “put two and two together” if they are bound by a strong tie. For example, investigations into the September 11 hijackings have revealed that various people in government understood different parts of the terrorist conspiracy, but because there were structural and legal limitations on their ability to communicate with each other, no individual had enough information to prevent the terrorist attacks from taking place.¹³⁴

B. Network Structure

Not all social networks are equally effective at transmitting information to their members. Network structure will reflect varying gradations of scale-free structure, and those variances may well be determinative with respect to whether information revealed at one node of a network makes its way to a distant node on the same network.¹³⁵

One critical structural variable is the prevalence of supernodes in a network, and the social distance from those supernodes to the periphery. Under a “strength of weak ties” analysis, we can see that the prevalence of supernodes who are weakly tied to multiple different close-knit communities will play a substantial role in determining how quickly and completely new information is disseminated through a society. All else being equal, a society solely interested in the rapid diffusion of stand-alone information will probably prefer for weak ties to exist between supernodes, as opposed to between peripherals.

and higher compensation”); Burt, *supra* note 91, at 6, 20, 24, 26, 33 (same benefits, plus supernodes’ ideas evaluated favorably within organizational hierarchy).

¹³¹ Daniel J. Brass, *Being in the Right Place: A Structural Analysis of Individual Influence in an Organization*, 29 ADMIN. SCI. Q. 518, 520, 532 (1984).

¹³² Tardy & Hale, *supra* note 91, at 353.

¹³³ Hansen, *supra* note 110, at 83, 105.

¹³⁴ NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, STAFF STATEMENT NO. 9, LAW ENFORCEMENT, COUNTERTERRORISM, AND INTELLIGENCE COLLECTION IN THE UNITED STATES PRIOR TO 9/11, at 3-5, 8-10 (July 26, 2004); Philip Shenon & David Johnston, *Threats and Responses: The Inquiry*, N.Y. TIMES, Oct. 2, 2002, at A17. See generally ROBERTA WOHLSTETTER, PEARL HARBOR: WARNING AND DECISION (1962) (discussing, inter alia, the failure of American intelligence and defense officials to connect the dots regarding the pending Japanese attack on Pearl Harbor).

¹³⁵ Cf. Amitai Aviram & Avishalom Tor, *Overcoming Impediments to Information Sharing*, 55 ALA. L. REV. 231 (2004) (discussing the sharing of information by competitors in network industries).

A second important structural variable is the extent of linkages in society. Supernodes can have functioning weak ties with 100 people, or weak ties with 2000 people. The greater the number of active linkages a supernode has, the better information will flow through a network. The same is true of a social networks' peripherals, and the "ordinary nodes" who fall somewhere in between supernodes and peripherals. *Ceteris paribus*, better-linked nodes mean more information transmission.¹³⁶ Indeed, this idea that links are essential is part of the basis for Robert Putnam's influential argument that social capital and robust associational activity help promote economic well-being.¹³⁷

The need for concealment of network activities from outsiders may also decrease the communicative efficiency of a social network. When the information at issue is highly sensitive, perhaps because it reflects illegal or politically disfavored motivations, network members will have to be quite cautious about sharing information. In such circumstances, weak ties may become totally inactive, as individuals begin sharing information only with well-trusted associates. Examples of such networks include criminal conspiracies, networks of political opposition in totalitarian regimes, and interaction networks in certain singles bars.¹³⁸

C. *Cultural and Strategic Considerations in Sharing*

Staying with the subject of concealment, sociological research shows that certain kinds of information are inherently more likely to be shared among members of a social network than other kinds of information. The better empirical studies of information sharing involve topics as diverse as HIV status, student discipline, and bakery closings.¹³⁹

¹³⁶ The extent to which all of a community's members are directly linked to each other is referred to as the network's "density." So imagine a network with 20 people. If each of these 20 people know all 19 of their fellow community members, then the network can be described as having high density. If, on the other hand, each of these 20 people knows only 3 or 4 of the other community members, then the network can be described as having low density. SCOTT, *supra* note 109, at 32. For further discussion of various measures of network structure, see Rowley, *supra* note 84, at 896-900.

¹³⁷ See ROBERT D. PUTNAM, *BOWLING ALONE* (2001) (describing the decline of social capital in the United States); ROBERT D. PUTNAM, *MAKING DEMOCRACY WORK* (1994) (comparing the wealth of social capital in Northern Italy to the dearth of social capital in Southern Italy and using the discrepancy to explain the south's relative impoverishment).

¹³⁸ See, e.g., Baker & Faulkner, *supra* note 129, at 854 (finding that "the need to conceal overrides the need for efficient coordination" in price-fixing conspiracies); Raymond A. Bauer & David B. Gleicher, *Word of Mouth Communication in the Soviet Union*, 17 PUB. OP. Q. 297, 309-310 (1953) (discussing the Soviet Union's attitude toward unofficial, unsanctioned word-of-mouth networks, and the behavior of participants in these networks); Carol Brooks Gardner, *Access Information: Public Lies and Private Peril*, 35 SOCIAL PROBLEMS 384, 386-94 (1988) (discussing women's reluctance to provide men with their correct names, addresses, and other identifying information in bars and other public spaces); Rowley, *supra* note 84, at 903 (characterizing a Colombian drug cartel's structure as centralized, and low-density).

¹³⁹ Other interesting and pertinent empirical work includes Laurel Richardson's study of sixty-five unmarried women who engaged in long-lasting adulterous relationships with married men. Richardson, *supra* note 8, at 209. Perhaps surprisingly, Richardson found that none of the women ever publicly revealed their affairs, and that it never occurred to them to do so. *Id.* at 213-14. Moreover, many of the women curtailed their conversations with third parties as a means of preventing themselves from "letting slip" information about their involvement with married men. *Id.* at 216.

A brief discussion of these three studies will help contextualize the lessons that can be drawn from the empirical literature on social networks.

1. HIV

Courts often treat HIV positive status as a presumptively private fact.¹⁴⁰ And yet, not surprisingly, virtually all people who are HIV positive disclose this information to at least *some people*.¹⁴¹ A 1995 study by Shelley, Bernard, Killworth, Johnsen, and McCarty interviewed a population of 70 HIV positive people to determine how widely information about them was known in their social networks.¹⁴²

The Shelley study revealed several interesting findings. First, there were many facts about the interviewees that were less widely known by friends, relatives, and acquaintances than their HIV status. HIV status was more widely known within the interviewees' social networks than their political party affiliation, their blood type, the presence or absence of a criminal record, their labor union membership, whether their home had been broken into in the past year, their approximate income, their religion, whether they'd served in the military, what the most important problems in their households were, major life events that had happened during the last 12 months, whether they had ever been shot or threatened with a gun, the amount of time they had lived at their current address, where they had traveled during the past twelve months, and several other facts.¹⁴³ There were relatively few facts about the interviewees that were more widely known than their HIV status: just their sexual preference, their real first name, whether they used illegal drugs, their number of children, their address, their birthplace, their age, their marital status, their work status, and their occupation.¹⁴⁴ To be sure,

A second study, by Loretta Stalans and Karyl Kinsey, looked at the information that audited taxpayers spread through their social networks. Loretta J. Stalans & Karyl A. Kinsey, *Self-Presentation and Legal Socialization in Society: Available Messages About Personal Tax Audits*, 28 L. & SOCIETY REV. 859 (1994). Most people who were audited did talk to others about the experience, and nearly one in four people talked to more than eleven people about the audit. *Id.* at 874. Auditees were most likely to talk to family members, then friends or neighbors, then co-workers. Stalans and Kinsey concluded that, for the most part, "stories about personal experiences that spread through social networks often provide a fair representation of the audit process and serve to correct media portrayal of auditors as primarily rude, punitive, and unfair." *Id.* at 890. There were, however, some distortions: Where auditees felt their integrity had been attacked during the audit process, or had been treated rudely but received favorable outcomes (i.e. no increased tax liability), they were quite likely to discuss the incompetence of the auditors and the slowness of the process with members of their social networks. *Id.* at 878-79, 890. As a result, messages reflecting rude treatment and auditor incompetence were over-represented in network communications, while polite treatment and auditor competence were under-represented.

¹⁴⁰ See, e.g., *Urbaniak v. Newton*, 226 Cal.App.3d 1128, 1140 (1991); *Doe v. High-Tech Institute*, 972 P.2d 1060, 1070 (Colo. App. 1998); *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491, 494 (Ga. 1994).

¹⁴¹ Gene A. Shelley et al., *Who Knows Your HIV Status? What HIV + Patients and Their Network Members Know About Each Other*, 17 SOCIAL NETWORKS 189, 211 (1995).

¹⁴² *Id.* at 189.

¹⁴³ *Id.* at 203 & 192. At least 17 facts about the interviewees were less widely known than their HIV status, approximately two facts were as widely known (health status, and education level) and 10 facts were more widely known. *Id.*

¹⁴⁴ *Id.* at 202.

someone's HIV status may be more pertinent than his blood type, and hence an individual may have more acquaintances who "need to know" his HIV status, but this data still suggests that people's HIV positive status is not a terribly closely guarded secret.

Second, the researchers found strong evidence of selective disclosure within the social networks of HIV positive individuals. Interviewees were much more likely to have disclosed their HIV status to members of organized support groups than to their relatives and friends.¹⁴⁵ Indeed, a number of HIV positive interviewees reported that they were reluctant to tell relatives, close friends, and even sexual partners about their HIV positive status because of the fear of stigmatization, abandonment, homophobia, job loss, or violence.¹⁴⁶ Disclosing HIV status to support group members, many of whom were themselves HIV positive, was seen as less threatening.¹⁴⁷ Reciprocity safeguarded the disclosures. Other studies of selective disclosure have found similar results in varied contexts.¹⁴⁸ There is a critical finding implicit in this data, although Shelley and his coauthors did not highlight it: HIV positive individuals disclosed their status to some members of their social networks while successfully keeping other members of their networks from discovering the information. Disclosure to a support group member did not make disclosure to other friends or relatives inevitable, even though those kept in the dark might have been highly interested in learning about the interviewees' HIV status.¹⁴⁹

Third, the researchers discovered that HIV positive individuals had unusually small social networks.¹⁵⁰ There were several factors contributing to this lack of links: Some HIV positive individuals were shunned by former friends and relatives; some withdrew from former friends and relatives as a way of sparing them the pain of death; many had seen their social networks shrink because of HIV-related mortality; and most interviewees were no longer working, which removed them from employment-related social networks.¹⁵¹ Moreover, the HIV positive people interviewed tended to behave like economically disadvantaged people do – they withdrew into small, close-knit

¹⁴⁵ *Id.* at 203-04.

¹⁴⁶ *Id.* at 194, 204-13.

¹⁴⁷ *Id.* at 204.

¹⁴⁸ *See, e.g.,* Baxter & Widenmann, *supra* note, at 324, 331 (finding that individuals were much more likely to conceal their romantic involvements from their parents than from their friends).

¹⁴⁹ There is evidence suggesting that closeted homosexuals consciously go to great lengths to make sure that the part of their social networks that know their sexual orientation do not intersect with the parts of their social networks that assume they are heterosexual. *See* Peter Davies, *The Role of Disclosure in Coming Out Among Gay Men*, in *MODERN HOMOSEXUALITIES: FRAGMENTS OF LESBIAN AND GAY EXPERIENCE* 75-81 (Ken Plummer ed. 1992).

¹⁵⁰ Shelley, *supra* note 141, at 200; *see also* WILLIAM CRAIG CARTER, *SOCIAL NETWORKS AND STIGMATIZATION* 14-19 (PhD Dissertation in Sociology at Louisiana State Univ.) (UMI Dissertation No. 9984316) (finding that HIV positive people, along with other stigmatized individuals, have smaller social networks).

¹⁵¹ Shelley, *supra* note 141, at 194, 199-200, 214.

communities comprised mostly of other HIV positive individuals, cutting off many weak ties with the outside world.¹⁵²

2. Girls' School Gossip

A second important study of information networks predates the advent of social network theory. In the mid-1950s, Stanley Schachter and Harvey Burdick studied the flow of gossip through a school for girls.¹⁵³ The researchers had teachers publicly remove one student from each of four classrooms, explaining out loud that the student would be gone for the rest of the day.¹⁵⁴ In the remaining classrooms at the school, no students were removed. The researchers then planted a rumor about the explanation for the students' removal with four student confederates, two of whom were in classes from which a student had been removed. A few hours later, following lunch and recess, all the girls in the school were interviewed to gauge what they had heard about the reasons for the four girls' removal.

The researchers reported several interesting findings. First, all but one of the 96 girls interviewed had heard the rumor in question.¹⁵⁵ Second, girls from whose classes a student was removed passed along the rumor to a significantly greater number of students, and spent more time discussing the rumor, than did those girls whose classes witnessed no disruption that morning.¹⁵⁶ Schachter and Burdick concluded on the basis of this data that there were far stronger incentives to discuss and transmit the rumor "when the issue to which it is relevant is important" to the audience and/or speaker.¹⁵⁷ Third, the planted rumor was not distorted substantially as it passed through the school's social network.¹⁵⁸ The story that the girls told the interviewers was essentially the same story that the researchers had planted that morning. Fourth, at least twelve alternative rumors relating to the girls' removal circulated through the school.¹⁵⁹ Students in classes that had witnessed a removal were much more likely to concoct new rumors and to discuss them with peers.¹⁶⁰ Moreover, students who were friends of the removed students tended to circulate rumors that cast them in a favorable light (i.e., "she's receiving an award") while students who were not friendly with the removed students

¹⁵² *Id.* at 214. Indeed, this correlation is not surprising, since so many of the HIV positive individuals interviewed were poor. *Id.* at 194.

¹⁵³ Stanley Schachter & Harvey Burdick, *A Field Experiment on Rumor Transmission and Distortion*, 50 J. ABNORMAL & SOCIAL PSYCHOLOGY 363 (1955). For a review of the Schachter and Burdick studies, as well as several other early studies of rumor transmission, see H. Taylor Buckner, *A Theory of Rumor Transmission*, 29 PUBLIC OPINION Q. 54, 65-70 (1965).

¹⁵⁴ Schachter & Burdick, *supra* note 153, at 365.

¹⁵⁵ *Id.* at 366.

¹⁵⁶ *Id.* at 368.

¹⁵⁷ *Id.*; see also KIMMEL, *supra* note 19, at 48.

¹⁵⁸ *Id.* at 370.

¹⁵⁹ *Id.* at 369.

¹⁶⁰ *Id.*

circulated rumors that cast them in a negative light (i.e., “she broke school rules and is being disciplined.”)¹⁶¹

3. Hong Kong Bakeries

A third study, by Gina Lai and Odalia Wong, looked at the spread of an untrue rumor through Hong Kong.¹⁶² The somewhat whimsical episode, and the data that Lai and Wong obtained about how the tale spread, revealed a great deal about how information gets transmitted through large, complicated social networks.

On November 24, 1997, several workers at a Hong Kong bakery chain saw fellow employees receiving layoff notices and evidently concluded that the chain was going bankrupt.¹⁶³ This belief was plausible enough, since during that same year a department store with which the bakery chain was previously affiliated had declared bankruptcy and closed all its stores.¹⁶⁴ In any event, the bakery shutdowns would have affected many consumers, as it is apparently common in Hong Kong for people to exchange bakery vouchers, which can be redeemed for baked goods.¹⁶⁵ With thousands of bakery vouchers in circulation, the rumor caused Hong Kong residents to rush to the bakeries, trying to redeem their vouchers before the stores closed. Within a few hours of the rumor’s origination:

thousands of (Hong Kong) people, upon hearing the news, brought all their vouchers (ranging from one to dozens) and rushed to the shops. . . . [T]hey pushed and squeezed into the shops and got whatever cakes or pastries [were] left. When all the cakes and pastries in the shops were taken, many people would even wait for hours outside the shops for new batches to come out. To calm down this mass hysteria, the [bakery] immediately made public announcements to clear the rumor in that

¹⁶¹ *Id.* at 369-70. Related studies suggest that people would be more likely to spread negative rumors about a girl to groups of students who had negative impressions of her, and positive rumors to students who had favorable impressions of her. E. Tory Higgins, *Achieving “Shared Reality” In the Communication Game: A Social Action that Creates Meaning*, 11 J. OF LANGUAGE & SOCIAL PSYCH. 107, 113-17 (1992); Charles Stangor et al., *Changing Racial Beliefs by Providing Consensus Information*, 27 PERSONALITY & SOCIAL PSYCH. BULLETIN 486, 493 (2001). There may have been a second-order effect here too, since people generally believe rumors whose truth they want to believe. Buckner, *supra* note 153, at 57; *see also* Gambetta, *supra* note 19, at 211 (“A convincing story gets repeated because of its appeal not its truthfulness.”).

¹⁶² Gina Lai & Odalia Wong, *The Tie Effect on Information Dissemination: The Spread of a Commercial Rumor in Hong Kong*, 24 SOCIAL NETWORKS 49 (2002). The run on baked goods that Lai and Wong describe is in many ways similar to standard runs on bank funds or currencies. *See, e.g.*, Barrie A. Wigmore, *Was the Bank Holiday of 1933 Caused by a Run on the Dollar?*, 47 J. OF ECON. HIST. 739 (1987). For another good study on rumor transmission in mass society, *see* J.N. Kapferer, *A Mass Poisoning Rumor in Europe*, 53 PUBLIC OPINION Q. 467 (1989).

¹⁶³ Lai & Wong, *supra* note 162, at 54.

¹⁶⁴ *Id.* at 53.

¹⁶⁵ *Id.* at 54.

evening. However, there were still people coming to the shops to redeem their vouchers the next day.¹⁶⁶

The rumor was totally unfounded, and yet it caused a complete breakdown in the generally orderly Hong Kong market for pastries.

Luckily, something good came out of the disturbance, as sociologists Lai and Wong were able to launch a telephone poll of 1011 respondents within a week of the event, asking Hong Kong residents how they learned about the rumor. By that time, more than 90% of the respondents had heard of the rumor.¹⁶⁷ Lai and Wong's data provides the most detailed analysis to date of how a rumor spreads through an urbanized society. I'll focus on a few of their more interesting findings.

First, informal social networks seem to have been vital in spreading the information. Many people heard about the rumor before it was reported in the mass media, and personal ties were the second most common source for hearing about the rumor (after television).¹⁶⁸

Second, only thirty percent of those who heard the information through personal ties passed the information on to others.¹⁶⁹ This suggests a tendency for information to *degrade* as it passes through a network. It will degrade in a predictable manner, not a random manner: People will pass along a rumor that they have heard if they perceive it to be new and non-redundant, interesting to the relevant audience, and credible. The Hong Kong data also suggests that there can be an opportunity cost of passing along new information – in this case slowing down one's dash to the bakery and increasing the odds of encountering a longer line upon one's arrival. Social networks thus function somewhat differently from the communications network associated with the childhood game, Telephone. Each player can choose whether or not to pass along the information to the next player, and we can expect that many rumors will never make their way through the entire social network.¹⁷⁰

Third, people tended to spread the rumor to members of their networks who they believed would benefit the most from the information.¹⁷¹ Thus, those surveyed were more likely to spread the information to people who they thought owned bakery vouchers.¹⁷² Because the vouchers are frequently given as gifts, we might have expected

¹⁶⁶ *Id.*

¹⁶⁷ *Id.* at 56-58.

¹⁶⁸ *Id.* at 54, 58.

¹⁶⁹ *Id.* at 59. Kapferer's study involved a rumor that a common food additive was toxic. Slightly more than half the people who heard this rumor reported passing it along to one or more people. Kapferer, *supra* note 162, at 476 tbl. 5. The most common response was discussing the rumor with other persons or showing others the leaflet on which the rumor circulated.

¹⁷⁰ Although Schachter and Burdick's rumor did spread to almost all of the girls at the school, the authors noted that this result was anomalous, driven to a substantial extent by the mysterious, unprecedented, and highly salient removal of four girls from classes for unspecified reasons. Schachter & Burdick, *supra* note 153, at 365, 368. Schachter and Burdick noted that in the vast majority of previous experimental studies of rumor transmission, the planted rumor barely spread through the studied population. *Id.* at 363.

¹⁷¹ See Buckner, *supra* note 153, at 64-65; see also Kimmel, *supra* note 19, at 94.

¹⁷² Lai & Wong, *supra* note 162, at 62.

reasonably high levels of awareness with respect to whether close associates might have vouchers. Moreover, because the information concerned shopping for food, which is predominantly done by women in Hong Kong, people were more likely to tell females about the rumor.¹⁷³

Fourth, those interviewed played some role in re-directing the information from weaker ties to stronger ties. Whereas more than 74% of interviewees heard the news from non-kin (typically co-workers), those interviewed passed the information on to a group that was comprised of 45% kin and 55% non-kin.¹⁷⁴ To the extent that kinship is a proxy for strong ties, this suggests that most people were more highly motivated to spread the potentially valuable information to those whose relationships they valued the most.¹⁷⁵ Further data backed up this assessment. Among those who heard the information through personal ties, 34% described their relationships with the informants as “very good,” 24% described them as “good,” and 41% described the relationships as “fair.” But those surveyed redirected the information to a different population: 52% of those who the respondents informed of the rumor had “very good” relationships with the respondents, 22% had “good” relationships, and only 26% had “fair” relationships.¹⁷⁶

Finally, the source of the information mattered – both the original source, and the identity of the immediate informant.¹⁷⁷ The rumor appeared to spread quickly, in part, because it was reported to have originated inside the company. And it also spread quickly because the rumor was passed on by people who had an incentive to be truthful – the sampled population was more likely to pass it along to people they cared about, and we know from other studies that information transmitted through strong ties tends to be more persuasive and influential than information transmitted through less reputable sources.¹⁷⁸

D. *Interaction Between Structure and Culture*

Synthesizing these insights about structure and culture can produce new insights that apply to information dissemination. For example, structure and culture combine to make it exceptionally unlikely that information about a private figure will be interesting beyond two degrees of separation. Duncan Watts notes that “anyone more distant than a friend of a friend is, for all intents and purposes, a stranger. . . . [A]nything more than two

¹⁷³ *Id.* at 62, 63.

¹⁷⁴ *Id.* at 67. This data suggests that a relatively small number of supernodes, mostly in workplaces, passed along the information to very large numbers of people. Thus, it appears that the communications network at issue here was scale-free.

¹⁷⁵ Other social network studies have suggested that in times of crisis, or extreme need, people are much more likely to rely on strong ties, especially kinship ties, than weak ties. Yossi Shavit, Claude S. Fischer, & Yael Koresh, *Kin and Nonkin Under Collective Threat: Israeli Networks During the Gulf War*, 72 SOCIAL FORCES 1197 (1994).

¹⁷⁶ *Id.* at 68 (data rounded to the nearest percent).

¹⁷⁷ Buckner, *supra* note 153, at 56 (noting that tying a rumor to a credible source increases the likelihood of its transmission); Kapferer, *supra* note 162, at 478 (same).

¹⁷⁸ KIMMEL, *supra* note 19, at 56; Ibarra & Andrews, *supra* note 100, at 282.

degrees might as well be a thousand.”¹⁷⁹ Watts’s argument that people have trouble seeing beyond two degrees of separation is true, but it is also the case that, at least in the pre-*Friendster* era, no one much cared about those people who were removed from us by more than two links.¹⁸⁰

An illustration will be helpful: Extra-marital affairs are fascinating events.¹⁸¹ That said, no self-respecting person would go to a cocktail party and tell a private story about a friend of a friend of a friend who is having an adulterous affair with someone unknown to the speaker and listener. It is only if the speaker or listener know who the adulterers are, or if the details of the affair are particularly sordid, humorous, or memorable that the information is likely to get disseminated further through the social network.¹⁸² And by the time the information makes it through this chain, it seems likely that the participants’ names would have dropped out of the story.¹⁸³ Thus, when dealing with events described via word-of-mouth, someone should have a reasonable expectation of privacy beyond two links in a social network. If *A* tells *B* something private about *A*, and *B* tells *C*, and *C* tells supernode *D*, who shares the information with the public, then *A* should have a reasonable expectation of privacy as against *D*, assuming that *A* has no direct connections to either *C* or *D*.

This rule of thumb appears to hold less strongly when one moves away from word-of-mouth communications. Indeed, the increased prevalence of email, blogging,

¹⁷⁹ WATTS, *supra* note 83, at 299-300. Diego Gambetta echoes this point in his discussion of gossip:

If [an object of gossip] were unknown gossip would be meaningless. This requirement has been widely acknowledged. “Known,” however, should be taken to mean that [the] object is relevant in some respect to both the transmitter and the receiver of gossip. They may not know [the] object personally, but know, say, that they will soon meet [him.] We are at times interested in the lives of persons we will never know personally, but only in so far as they are friends of friends of friends. The more remote the link with [the] object, the more speculative gossip’s motives, which ultimately pale into a near-universal curiosity for human quirks.

Gambetta, *supra* note 19, at 205. This trend is a good thing, to the extent that we are concerned about the accuracy of gossip and other forms of accurate information. With each retelling of a story to someone an additional degree of separation from the subject, the story becomes increasingly inaccurate, portraying the subject in an increasingly extreme manner. See Tomas Gilovich, *Secondhand Information and Social Judgment*, 23 J. OF EXPERIMENTAL SOCIAL PSYCH. 59, 64-73 (1987).

¹⁸⁰ Friendster is an-Internet based program that produces maps of its members’ social networks, facilitating networking among members. It has proved particularly popular as a dating network, with individuals examining the profiles of their friends’ friends for attractive matches. See <<http://www.friendster.com>>.

¹⁸¹ Allport & Postman, *supra* note 129, at 509.

¹⁸² See *id.* at 502-05, 512-14; *supra* text accompanying notes 156 and 160.

¹⁸³ *Id.* at 505. For a terrific study of how pertinent information gets dropped from a story as it is sequentially retold by several individuals, see Anthony Lyons and Yoshihisa Kashima, *The Reproduction of Culture: Communication Processes Tend to Maintain Cultural Stereotypes*, 19 SOCIAL COGNITION 372 (2001). Lyons and Kashima found that aspects of a story that reinforced existing stereotypes about athletes were more easily recalled, and hence more likely to be repeated as the story passed through a chain of people, than stereotype-incompatible information. *Id.* at 385. See also KIMMEL, *supra* note 19, at 91-93 (describing more generally how rumors change when they’re transmitted through multiple links in a social network); Labianca, Brass, & Gray, *supra* note 119, at 64 (suggesting that rumors tend to get exaggerated when they circulate in social networks).

and other new forms of communications in recent decades has facilitated the more rapid dissemination of new information and created new categories of potential supernodes.¹⁸⁴ Thus, particularly embarrassing emails or memoranda have on occasion made their way around the world, even though few of the eventual recipients were familiar with the original parties to the communication.¹⁸⁵ The same is true of photographs or videos depicting private scenes, such as nudity or sexual conduct.¹⁸⁶ That said, the percentage of emails that get forwarded beyond two degrees of separation from the initial recipient must be so low as to render this risk the kind that a prudent private figure should ignore.¹⁸⁷ Moreover, so many emails flow into people's inboxes that the likelihood of any particular message being singled out for widespread dissemination is usually negligible.¹⁸⁸ Noise has long been an important method of protecting privacy.¹⁸⁹

The presence of legal or moral constraints on subsequent disclosure of information does (and ought to) inform a plaintiff's reasonable expectation of privacy in particular information too.¹⁹⁰ Obviously, a plaintiff has a reasonable expectation of

¹⁸⁴ KIMMEL, *supra* note 19, at 205; Uwe Matzat, *Academic Communication and Internet Discussion Groups: Transfer of Information or Creation of Social Contacts?*, 26 SOCIAL NETWORKS 221, 245-47 (2004); Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 119-120 (1995).

¹⁸⁵ See, e.g., Jonathan D. Glater, *Legal Research? Get Me Sushi, with Footnotes*, N.Y. Times, Oct. 22, 2003, at A1 (quoting from a now infamous research memo about the relative merits of Manhattan sushi restaurants, prepared at the direction of an attorney at Paul Weiss); Shaun Waterman, *Analysis: Clock-Forward Morality*, United Press International, Mar. 3, 2003, available in <<http://www.upi.com/view.cfm?StoryID=20030303-023031-9883r>> (visited May 26, 2004) (describing an off-the-record email that a journalist, Laurie Garrett, sent to a dozen friends, which was subsequently forwarded around the world and dissected on various blogs); The National Debate, *Paul Kelly Tripplehorn, Jr.: Your Fifteen Minutes Is Up*, July 15, 2003, available in <<http://www.thenationaldebate.com/blogger/articles/HutchisonInternEmail.htm>> (visited May 26, 2004) (describing reactions to an infamous break-up email sent from one Senate intern to another, and subsequently forwarded to thousands of people).

¹⁸⁶ See Ian Ith, *Local Porn Business Tries to Stay Under Wraps; Hilton Tape Bringing Unwanted Attention*, SEATTLE TIMES, Nov. 20, 2003, at B1 (describing the dissemination of an amateur sex tape showing Paris Hilton's escapades); Cf. *Lovisi v. Slayton*, 539 F.2d 349 (4th Cir. 1976) (involving a sodomy prosecution of participants in a ménage à trois, where the sex act came to light after the daughter of a participant discovered Polaroid photographs depicting the act and brought them into school).

¹⁸⁷ This is different from being forwarded twice, which is more common. By two degrees of separation, I mean that the recipient of a forwarded email knows neither the recipient, the sender, nor anyone who knows the recipient or sender, nor anyone who knows someone who knows the recipient or sender.

¹⁸⁸ When information overload occurs, interesting information might not be identified as such. As a result, information that would otherwise be passed along from one node to another never gets transmitted and remains obscure. On information overload, see KIMMEL, *supra* note 19, at 213; Matzat, *supra*, at 226.

¹⁸⁹ Prior to the development of modern communications technologies, individuals wishing to have a "private" conversation might have met in a private space, like a home, or a deserted warehouse. Alternatively, they might have gone to a crowded pub, where the chatter of fellow patrons created enough of a din to preclude effective eavesdropping.

¹⁹⁰ Diane Leenheer Zimmerman, *Secrets and Secretiveness: Patterns in the Fabric of the Law*, 78 CAL. L. REV. 515, 531 (1990) (reviewing KIM LANE SCHEPPELE, *LEGAL SECRETS, EQUALITY, AND EFFICIENCY IN THE COMMON LAW* (1988)) ("[B]reach of confidence clearly has teeth in that it affects how cases are decided. When information is obtained through a confidential relationship, courts allow disclosure only under extraordinary circumstances.").

privacy in the privileged information that he reveals to his attorney. Barring a malpractice suit, the client can expect that the information will remain confidential. But in certain cases, there will be no clearly established legal duty directing the person to whom information is disclosed. Suppose a famous actress attends an Alcoholics Anonymous meeting and says, “Hello, My name is Lara Flynn, and I’m an alcoholic.”¹⁹¹ There are evidently no legal or contractual constraints on the ability of those who attend Alcoholics Anonymous meetings to disclose what they heard.¹⁹² But Alcoholics Anonymous apparently share deeply held social norms barring the disclosure of information about attendees outside of the group setting.¹⁹³ If these norms are sufficiently powerful and almost universally adhered to by those who attend Alcoholics Anonymous, even where attendees are public figures, then the actress ought to have a reasonable expectation of privacy in the disclosed information. In short, certain groups can be designed to trigger reciprocal non-disclosure, and people making germane disclosures within these settings generally ought to expect that the information disclosed will not circulate outside the group.

E. Predictive Social Network Analysis

In 1977, Bernard Russell, Peter Killworth, and Lee Sailer articulated a lofty goal for social network analysis. They noted that a useful theory of information diffusion “must be able to predict how information flows through the system, how quickly it will go from point A to point B, and how likely it is to be trapped in pockets and loops.”¹⁹⁴ Twenty-seven years later, perfect predictability of information diffusion has not been achieved. This literature still has quite a ways to go, and would benefit from collaborative work that can shed light on the legal applications of information diffusion and social network theories. That said, there are several lessons from the literature that might help us predict with reasonable accuracy whether subsequent dissemination will follow initial disclosure. More precisely, information will or will not be disseminated through a social network depending on these factors:

- The structure of a network (Prevalence of ties and supernodes, mix of strong and weak ties, proximity of disclosure to a supernode, the difficulty of aggregating complex information through weak ties, the concealment versus efficiency tradeoff in network structure, and the extent to which technologies used by members of a social network facilitate or constrain information dissemination).

¹⁹¹ The National Enquirer has reported on celebrity participation in Alcoholics Anonymous meetings in the past. See, e.g., *Lara Flynn Boyle in Alcoholics Anonymous*, NATIONAL ENQUIRER, Mar. 20, 2003, available in <http://www.nationalenquirer.com/stories/feature.cfm?instanceid=57345> (visited May 23, 2004).

¹⁹² Bree Schonbrun, Comment, “*In the Light of Reason and Experience*”: *The Scope of the Evidentiary Privilege in the Self-Help Setting: Alcoholics Anonymous Examined*, 25 CARDOZO L. REV. 1203, 1225 n. 124, 1237-38 (2004). Nor are communications within twelve-step groups privileged. *Cox v. Miller*, 296 F.3d 89, 111-12 (2d Cir. 2002).

¹⁹³ *Cox*, 296 F.3d at 111-12; Schonbrun, *supra* note 192, at 1225 n.124.

¹⁹⁴ Bernard H. Russell et al., *Summary of Research on Informant Accuracy in Network Data, and on the Reverse Small World Problem*, 4 CONNECTIONS: BULLETIN OF THE INTERNATIONAL NETWORK FOR SOCIAL NETWORK ANALYSIS 11, 18 (1977).

- The cultural variables (Differentials in willingness to disclose facts to particular groups or types, the presence of moral or legal constraints on disclosure, network participants' ability to know which information other network members are likely to deem relevant, the propensity of certain information is likely to degrade as it passes through a network, and whether the information is of the type that is ordinarily transmitted through strong or weak ties).

Many of these variables will in turn depend on the nature of the information itself. Stand-alone information is efficiently transmitted through weak ties, but complex information cannot be aggregated and analyzed effectively through weak ties. People try to pass along information that will be particularly valuable to a recipient, based on their own awareness of the recipients' traits. Information about bakery closings will flow toward people interested in that subject matter and away from people unlikely to hold bakery vouchers. AIDS support group members may feel morally bound to avoid disclosing a fellow members' HIV positive status to a stranger, but may disclose the information freely upon learning that the stranger is himself HIV positive. In short, structural and cultural factors make it impossible to judge the *ex ante* likelihood of information transmission through a network without knowing the content of the purportedly private information. Interestingly, privacy doctrine *essentially ignores* the nature of the information itself in determining whether a plaintiff who has disclosed it to some people retained a reasonable expectation of privacy.¹⁹⁵

¹⁹⁵ Recall that the foundational privacy tort – public disclosure of private facts – has four elements: The defendant must (1) give publicity (2) to a matter concerning the private life of another (3) that is not of legitimate concern to the public (i.e., it is non-newsworthy), and the disclosure must be (4) highly offensive to a reasonable person. RESTATEMENT (SECOND) OF TORTS § 652(D) (1977). Privacy law thus disaggregates the question of “privacy” from the question of whether the information is “of legitimate concern to the public.” But as the foregoing analysis suggests, the privacy of facts and the public interest’s in those facts are *inherently connected*. Information that has been disclosed to at least one person is more likely to be disseminated further if members of the public will be interested in the information. *See supra* text accompanying notes 156 and 172-174. If I tell you that I had a bowl of cereal for breakfast this morning, I can expect that this information will not be disseminated further because it is so trivial that no normal person would repeat it to others. If, on the other hand, I tell you that I watched Peter Singer eat bacon for breakfast this morning, that information would be more likely to transmit itself through a social network, because it would reflect the possible hypocrisy of a famous vegetarian and animal rights advocate.

There is a dispute among the courts with respect to the meaning of the “not of legitimate concern to the public” prong of the public disclosure tort. Is this element descriptive? Or is it normative? Are courts asking what the public is likely to find interesting? Or are courts asking what information the public has the right to know? *See SOLOVE & ROTENBERG, supra* note 82, at 108, 100; Geoff Dendy, Note, *The Newsworthiness Defense to the Public Disclosure Tort*, 85 KY. L.J. 147, 157-64 (1996-97). The privacy case law splits on this question, with some courts deferring to news media defendants’ judgments about what information is newsworthy, *see, e.g.,* Neff v. Time, Inc., 406 F. Supp. 858 (W.D. Pa. 1976), and others holding that information is non-newsworthy, even though tens of thousands of individuals are willing to pay substantial sums of money to obtain the information. *See, e.g.,* Michaels v. Internet Entertainment Group, 5 F. Supp. 2d 823 (C.D. Cal. 1998). In my view, courts should ask *both* questions. They should ask whether the public is interested in this information as part of the determination of whether the plaintiff had a reasonable expectation that the information would remain private. They should ask whether the public ought to be entitled to see the information under the “legitimate concern to the public” prong of the public disclosure tort.

F. Lessons

We have seen that weak ties generally do a poor job of aggregating non-redundant information that is possessed by multiple nodes on a network. Thus, instances in which scattered private information about an individual is pieced together, and the aggregated information is disclosed, can be expected to be rare.¹⁹⁶ Where this information aggregation occurs through multiple sources linked via weak ties, we can write it off as a fluke that a reasonable person should have disregarded. By contrast, when scattered bits of private information exist within a close-knit network of people linked by strong ties, aggregation of that information is much more likely, and the plaintiff's expectation of privacy with respect to the aggregated information ought to be low.

We also have seen that the more interesting a particular piece of private information, the less likely it is to degrade as it passes through a network. Thus, if private information involves a highly unusual or surprising event, a well-known public figure, or relates to an important current event or trend, it is more likely to be disseminated through a network. Monica Lewinsky can expect greater privacy in her revelation to Linda Tripp that she is having an affair with Joe Schmo than she should in her revelation that she is having an affair with the President of the United States. Relatedly, once interesting information reaches a supernode, the supernode is more likely to deem the information worth sharing with her many contacts. And information that can be traced to an inherently credible source, such as a bakery employee at a store rumored to be closing, is also more likely to be disseminated through a network by people seeking to help out their peers. As a general matter, then, a plaintiff ought to expect that if he discloses previously private information that is likely to be regarded as highly interesting, novel, revealing, or entertaining, that information is rather likely to be disseminated. And, as in most privacy cases,¹⁹⁷ where it is the plaintiff who has made the initial disclosure of damaging information, the plaintiff ought to understand that his involvement at the story's origin made it more likely that the story would spread.¹⁹⁸

IV. Reading the Case Law in Light of Social Network Theory

Let us return to the tort law discussed in Part II. Some opinions hold that because the plaintiff has disclosed the information to a few people, she can no longer recover on the basis of a subsequent disclosure. Most opinions reach a contrary result, holding that a

¹⁹⁶ This discussion applies to information that has been transmitted through face-to-face interactions or telephone conversations. When information is communicated via the Internet or other archived communications media, new technologies like Google might make aggregation of scattered information a relatively simple matter.

¹⁹⁷ But not all. There are privacy cases in which the source of the information about an individual is a third party, not the plaintiff. Indeed, in some instances, third parties such as credit reporting agencies, health care providers, employers, or educators may have access to information about the plaintiff that he himself does not have. For example, an employer might improperly disclose to a third party confidential employment evaluations that the plaintiff has never seen.

¹⁹⁸ Cf. Runge & Archer, *supra* note 8, at 360 (noting that people assume that individuals are somewhat less likely to disclose private negative information about themselves than private positive information about themselves).

limited disclosure of private information by the plaintiff doesn't necessarily render that information "public" for the purposes of the privacy torts. There is, in short, substantial uncertainty with respect to how much disclosure can occur before the information becomes "public." Judges appear to be applying an ad hoc, "I know it when I see it" standard to reasonable expectations of privacy. This raises the natural question of how well courts' intuitive judgments comport with the social network findings discussed in the previous section. This Part addresses that question.

Before I do that, let me say a few words about what it means for something to become "public." In the cases that follow, I will assess publicity as the likelihood of the previously private information at issue reaching the people from whom the plaintiff would like to keep it. In some cases, like *Kubach*, that means people who have no relationship to the plaintiff. In other cases, like *Fisher*, that means people who have strong ties to the plaintiff. So at what point has a fact crossed over from private to public? Surely the test for public information cannot be whether a majority of the American public is aware of the information.¹⁹⁹

Perhaps social network theory can be used to provide a more attractive answer. One preoccupation of social network theorists has been to determine the size of an individual's social network. Although the studies vary somewhat, it appears that the median adult has met or otherwise interacted with approximately 1700 people.²⁰⁰ This does not mean that the average person has 1700 active ties, but rather that he "knows" roughly this number of people.

We can use this 1700-person threshold to establish the most liberal acceptable definition for public facts. If a fact about me is known by everyone with whom I am acquainted, as well as a few people with whom I am not acquainted, then that fact must be public under any meaningful conception of publicity. If, on the other hand, a particular fact is known by my friends, but not by any strangers, then I might argue that I retain an expectation of limited privacy in it. To determine whether someone has a reasonable expectation of privacy in information, we therefore might evaluate the possibility that the information will be disseminated to a number of people that exceeds the size of his social network.²⁰¹ If there is a low risk of such dissemination (e.g., lower than 5%), the courts can recognize a reasonable expectation of privacy.

The idea behind this approach, in short, is to assume that a plaintiff had perfect information about the risks of various outcomes at the time of his initial disclosure, and then assess whether those risks were sufficiently remote to justify the plaintiff's decision to disregard them. We assume that the plaintiff is fully informed about what might happen, but not about what will happen. We then use this calculus to evaluate whether it was reasonable for the plaintiff to proceed with the disclosure and assume that the

¹⁹⁹ If that were the test, then facts such as the identity of the House Minority Leader or the capital of Canada would be deemed private with respect to the United States population.

²⁰⁰ Peter D. Killworth et al., *Two Interpretations of Reports of Subpopulation Sizes*, 25 SOCIAL NETWORKS 141 (2003); Peter D. Killworth et al., *Estimating the Size of Personal Networks*, 12 SOCIAL NETWORKS 289 (1990).

²⁰¹ Most states hold that public disclosure of private facts requires the defendant to give widespread publicity to the facts in question. In most states, and under the Restatement, disclosure to a small group is not generally tortious, even if that small group has a special relationship with the plaintiff. A few states disagree. See SOLOVE & ROTENBERG, *supra* note 82, at 98-101.

information would remain obscure.²⁰² Because social networks tend to be scale-free, this analysis should often direct our attention to the proximity of a disclosure to a supernode. Widespread dissemination frequently will depend on the ex ante likelihood of particular information reaching a supernode and being disseminated further via that supernode.

Disclosure to a supernode will not only increase the number of people who will be exposed to the information at issue. It will also enhance the likelihood that the information will “jump” across a structural hole that otherwise separates two distinct sub-networks. Through supernode activities, information that the plaintiff did not mind sharing with members of his twelve-step group might find its way into a network of dentists, professors, secretaries, or – worst of all – tabloid reporters. In a tort suit, courts are always called upon to examine causation: Would the plaintiff have been harmed in the absence of the defendant’s actions? Social network theory provides a basis for evaluating that question when the plaintiff’s injury stems from dissemination of previously private information. Courts simply need to ask themselves: Was the widespread dissemination of this information inevitable, or did the defendant’s actions materially affect the extent of subsequent disclosure?

A. *Evaluating the Leading Cases*

Recall that *Sanders v. ABC* involved a conversation between two co-workers, within earshot of other co-workers at a telephone psychic business. The problem, from the plaintiff’s perspective, was that Lescht, one of the co-workers involved in the conversation, was actually a journalist undercover. There was an obvious dispute in this case about whether the communication between Sanders and Lescht was consensual and, as I suggested in Part I, social network theory provides little direct help there.²⁰³ Sanders might well argue that the journalists’ misrepresentations elicited from him information that he would have never revealed otherwise. And, of course, had Sanders known he was being interviewed on the record by a journalist producing a news clip, then he could not possibly have had a reasonable expectation of privacy in the information he revealed. A journalist, working in her employment capacity, is the most extreme version of a supernode, weakly tied to all her readers, viewers, or listeners.

²⁰² This analysis should apply to the plaintiffs’ conduct taken as a whole, not to a specific instance of disclosure. Thus, assume that there is a 1% chance of widespread dissemination every time Bill tells someone about his extramarital affair with Monica. If Bill tells only one friend about the affair, he might well have a reasonable expectation of privacy in the information. But if Bill tells 100 friends about the affair, he should not expect that the information will remain private.

²⁰³ For interesting discussions of these issues involving undercover journalists, compare *Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971) (recognizing an expectation of privacy) to *Desnick v. ABC*, 44 F.3d 1345 (7th Cir. 1995) (refusing to recognize an expectation of privacy).

Social network analysis may have something to contribute to this analysis. We are generally better able to determine whether someone is a supernode or peripheral if they are closely tied to us than if they are weakly tied to us. Bondonio, *supra* note 91, at 301. One could argue, therefore, that if the discloser and disclosee are closely tied, the disclosee’s actual status as a supernode or peripheral ought to be determinative. If, by contrast, they are weakly tied, and if society wants to encourage communication between weakly tied individuals, then the discloser was entitled to rely on the disclosee’s statement that he was an ordinary telephone psychic (likely to be a peripheral) and not a journalist (a supernode by definition).

Social network theory remains pertinent, however, because ABC defended its reporters' actions by arguing that as a matter of law what was said within earshot of fellow employees could not have been private. According to the court, Sanders told Lescht "about his personal aspirations and beliefs and gave Lescht a psychic reading."²⁰⁴ This is rather vague, but secondary media reports suggested that ABC broadcast a six-second clip of Sanders stating that he had previously worked as a stand-up comedian and implying that he was not a particularly motivated telepsychic.²⁰⁵ Suppose five or ten co-workers overheard these statements. The odds of them having disseminated the information to others were rather low, and the odds of this information having been disseminated beyond the circle of people who knew Sanders personally were essentially nil. Even if this stand-alone information had reached a supernode, no self-respecting supernode would risk the ire of her weak contacts by passing along such trivial information about a private figure.²⁰⁶ It is unsurprising that some telephone psychics are skeptical about the soothsaying enterprise, and the fact that one obscure psychic previously worked as a comedian borders on the inane. In holding that the presence of co-workers did not render the communication public, the *Sanders* court reached a result that is both intuitive and consistent with the social science.²⁰⁷

Kubach v. Multimedia WMAZ,²⁰⁸ raised the more difficult question of whether an individual's disclosure of his HIV status to sixty friends, relatives, support group members, and health care professionals rendered that information public for the purposes of privacy law. The Georgia Supreme Court held that the information remained private. Obviously, much of the disclosure to health care providers would be protected by a doctor-patient privilege, duties of confidentiality, and substantive regulations such as the Health Insurance Portability and Accountability Act²⁰⁹ and so these disclosures would hardly render the information public. But what about non-privileged disclosures to

²⁰⁴ 20 Cal.4th at 907.

²⁰⁵ Jane Kirtley, *Cracking Down on Covert Media Taping*, AM. JOURNALISM REV., Sept. 1999, available in http://www.ajr.org/article_printable.asp?id=3198 (visited June 30, 2004). I'm working on tracking down a transcript of the broadcast.

²⁰⁶ ABC only broadcast the information because it led color to a more substantive news story about scams within the telephone psychic industry. ABC never would have broadcast this clip as the basis for a stand-alone news piece, especially not during February, when the piece aired. (February is a Nielsen sweeps month.)

²⁰⁷ The primary California case delineating the limits of limited privacy seems to have been rightly decided under network theory too. In *Sipple v. Chronicle Publishing Co.*, 154 Cal.App.3d 1040 (1984), discussed *supra* note 51, the court implicitly held that once hundreds of homosexuals in several cities knew of Sipple's sexual orientation, and once Sipple's heroic actions to thwart the attempt on President Ford's life thrust him into the national limelight, then it was inevitable that Sipple's orientation would spread from the social network of homosexuals to the social network of heterosexuals. This analysis is convincing, and we might further expect that the "mainstreaming" of homosexuality since 1984 has increased the number and intensity of links between gays and straights. For empirical analysis of network ties between gays and straights, see WILLIAM EDWARD WAGNER, *IDENTITY MANAGEMENT AND THE SOCIAL NETWORKS OF GAY PROFESSIONAL MEN* (Dissertation Abstracts International, A: Humanities and Social Sciences) 2003, 63, 12, June, 4491-A.

²⁰⁸ 443 S.E.2d 491 (Ga. 1994).

²⁰⁹ See 45 C.F.R. § 160-164. The Act is better known by its acronym – HIPAA.

friends, relatives, and support group members? The Shelley et al. study of HIV disclosure suggests that information about HIV status is frequently shared with some parts of an individual's social network, while other members, who might know the HIV positive person well and be interested in her health status, remain in the dark.²¹⁰ Information about HIV status, therefore, seems not to flow through social networks readily, at least in the case of private figures.²¹¹ Although this particular fact was far more interesting, inherently, than the facts at issue in *Sanders*, and although the information was again stand-alone, Kubach had a reasonable expectation that his disclosure to some people who knew him would not result in the information being revealed to others who knew him, let alone thousands of people in his local community. So the court got this harder case right too.

It is less obvious whether the court reached the right result in *Y.G. v. Jewish Hospital*.²¹² Again, set aside the consent issue of whether the plaintiffs could have done more to avoid being filmed. The G. family went to a party attended by similarly situated couples in their local community, and were horrified when their attendance became known to members of their church and the husband's co-workers. The defendants argued that by going to this large party with forty attendees, the G.s lost any expectation that their participation would remain private.

Evaluating this claim is difficult, especially since there has not been an empirical study similar to the Shelley study conducted to discern knowledge of in vitro fertilization participation within couples' social networks. So we will have to extrapolate from what we do know. The G. family's participation in the program, combined with their membership in a church that condemned in vitro fertilization, amounted to complex information. Such information would be unlikely to be aggregated via weak ties. Hence, if the G.s went to the party and disclosed to no one there that they belonged to a church that condemned in vitro fertilization, then they should have a rather strong expectation of privacy. Moreover, the objections of that church notwithstanding, there appears to be less stigma associated with in vitro fertilization or infertility generally than there is for HIV positive status. The hospital's decision to invite a television crew to the party, and the other attendees' evident lack of objection to its presence provides at least weak inferential evidence in support of that view. From this it follows that there would be fewer moral constraints among the people at the party against subsequent disclosure but also less interest in spreading that information. Moreover, anyone in attendance at the party, other than the TV crew, would have been a health care provider (with a duty of confidentiality) or a fellow participant in the program. Fellow participants who belonged to the same church, if any, would have been prevented from disclosing information about the G.'s participation to fellow church members by a fear of symmetrical disclosure by the G.s. At the same time, it appears that the hospital was located in the G.'s local community, and their odds of being recognized by someone from their church or workplaces were therefore heightened.

²¹⁰ See *supra* text following note 148.

²¹¹ The same may be true of celebrities. See Barbara Liss, *The Public and Private Rock: Two Views of the Late Star*, HOU. CHRON., July 13, 1986, at 15 (discussing Rock Hudson's role in the disclosure of his previously private HIV status just two months before his death).

²¹² 795 S.W.2d 488 (Mo. Ct. App. 1990).

In short, the court's determination that the information was not public is at least defensible, and probably right, but ideally the court would have investigated (a) whether the G.'s statements at the party transformed previously complex information into stand-alone information (i.e., whether they disclosed both their identities and their church's objections to the procedure); and (b) whether the G.s spent much time talking to other party attendees and sharing identifying information.²¹³

Duran v. Detroit News, Inc.,²¹⁴ by contrast, is a case where the court's analysis cannot be squared with social network theory. Recall that Duran was a former Columbian judge who had battled Pablo Escobar's drug cartel. According to the court, Duran used her real name when shopping in stores or eating in restaurants, which waived an expectation of privacy in her identity. Under a network theory approach, these acts, combined with her notoriety in Columbia, would not have eliminated her reasonable expectation of privacy in her identity. Shopping in a store or eating in a restaurant involves weak-ties interactions. At most, Duran would have come into fleeting contact with other customers or service sector employees. There was nothing interesting about Duran's shopping or eating out. In order to generate interest in the story, the defendant had to connect Duran's presence in Detroit to her past notoriety in Columbia and the bounty that had been placed on her head. Such information was quite unlikely to be aggregated through the kinds of weak ties that Duran established in Detroit's public spaces. Perhaps a Columbian waiter put two-and-two together, but this would have been a highly improbable turn of events. Duran's general obscurity in Detroit properly engendered a reasonable expectation of privacy with respect to her shopping and visiting restaurants.²¹⁵

*Nader v. General Motors*²¹⁶ presents a closer case. General Motors was interested in obtaining information about Nader's sexual proclivities, political and religious beliefs, and views regarding race relations. Its agents therefore interviewed Nader's close friends and business associates under false pretenses. These acts raised the question of whether the interviews amounted to an intrusion upon Nader's seclusion. The court found no intrusion upon seclusion, but it is difficult to answer this legal question in the abstract. Nader was a public figure, and so there was a heightened probability that information he revealed to friends and associates eventually would have been disclosed to the public at large.²¹⁷ That said, the likelihood of disclosure would depend on the extent to which the information at issue was interesting or surprising, and the existence of any moral

²¹³ I have contacted the attorney who represented Y.G., but he has not responded to my request for more information about the case.

²¹⁴ 504 N.W.2d 715 (Mich. Ct. App. 1993).

²¹⁵ Duran's disclosure to her neighbors that she had been threatened by drug dealers, however, may be a different story. Particularly given the size of the bounty at issue, one wonders whether the dissemination of Duran's identity (if not to the public at large, then at least to Escobar's cartel) became rather probable if she shared with her neighbors a detailed account of her tribulations. Unfortunately, the court's opinion is quite vague with respect to the details of these disclosures.

²¹⁶ 255 N.E.2d 765 (N.Y. 1970).

²¹⁷ Statements that would be unremarkable if uttered by a private figure can be remarkable if uttered by a public figure. An office worker's use of an expletive is totally unremarkable, but the vice-president's use of the same word is front-page news in the paper of record. See Richard W. Stevenson, *Cheney Owns up to Profanity Incident and Says He "Felt Better Afterwards,"* N.Y. TIMES, June 26, 2004, at A1.

constraints on the disclosure of such information. Simply put, one needs to know the details of Nader's sexual proclivities, political and religious beliefs, and racial attitudes in order to determine whether he possessed a reasonable expectation of privacy against subsequent disclosure of them to third parties.

Social network theory even helps us understand the numerically puzzling result in *Fisher v. Ohio Department of Rehabilitation and Correction*,²¹⁸ where the plaintiff's disclosure of information to three co-workers rendered it non-private as a matter of law. Recall that the information at issue there involved sexually charged encounters between a mother and her seven-year old son. At least in the United States, such information is so inflammatory that it is unlikely to remain bottled up in an office environment that includes large numbers of strong ties. In most American workplaces, people tend to meet their co-workers' spouses. Given the likelihood of at least weak ties between office workers and the plaintiff's husband, disclosure to him was probable, if not inevitable. While additional facts about the relationships among Fisher, her former spouse, and her co-workers would have been helpful, the court's categorical determination is defensible in light of the salaciousness and possible illegality reflected in the plaintiff's disclosures.

B. Judges or Juries?

In the cases discussed above, appellate court judges examined whether the plaintiff's disclosure of previously private information rendered that information public as a matter of law. In cases where the court answered that question in the affirmative, the plaintiff's privacy claims were dismissed. But in those cases where the court answered that question in the negative, the plaintiff's privacy claims were submitted to the finder of fact. Essentially, the trial judges were holding that the information at issue could be private, and letting the jury decide whether it was in fact private.

In both *Sanders* and *Kubach*, juries ultimately found that the defendants had publicized private information. The *Sanders* jury awarded the plaintiff \$635,000,²¹⁹ and the *Kubach* jury awarded the plaintiff \$500,000 in compensatory damages and \$100 in punitive damages.²²⁰ Thus, the jurors' conception of privacy tracked the results that are consistent with social network theory. In *Y.G. v. Jewish Hospital*, the court remanded for a jury trial, but shephardizing the case reveals nothing about what happened on remand, and the local media stopped covering the story after the appellate court published its opinion.²²¹ In *Fisher*, the trial court properly concluded that the plaintiff's disclosure of her Oedipal thoughts regarding her young son was likely to result in her estranged husband's learning this salacious information. Maybe the likelihood of disclosure was 50% or maybe it was 15%, but armchair social network analysis suggests that no reasonable juror could find a very low likelihood of disclosure to the husband. The court's decision to prevent the issue from going to the jury was defensible.

²¹⁸ 578 N.E.2d 901 (Ohio Ct. Cl. 1988).

²¹⁹ See *supra* text accompanying note 50.

²²⁰ 443 S.E.2d 491, 495 (Ga. 1994).

²²¹ Andre Jackson, *Newsworthy or No One's Business?: 2 in Fertility Program Sue over TV; Publicity*, ST. LOUIS POST-DISPATCH, July 23, 1990, at 1B.

In the other cases discussed above, *Nader*, and *Duran*, the courts similarly removed from the jury the opportunity to determine that information that the plaintiff had shared with some people nevertheless remained private. For the reasons stated above, although *Nader* reached a result that may well have been correct under social network theory, it presented a sufficiently close question to warrant resolution of the issue by the finder of fact. Jurors could hear evidence about the facts of the case, as well as expert testimony from sociologists skilled in social network theory to help them evaluate the likelihood that the information in question would have been disseminated widely in the absence of the G.M.'s involvement. In *Duran*, by contrast, it seems that no reasonable juror could have concluded that the plaintiff's use of her name in restaurants would enable someone to connect her to the Columbian drug cartel, and it would have been appropriate for the court to hold that the former judge's identity and the threats against her were private as a matter of law.

There is an alternative approach. Although it should be much easier for jurors to apply social network theory in privacy disputes than economic theory in antitrust cases or cutting edge scientific principles in patent suits, we might still worry that jurors will prefer to rely on their own intuitions rather than the social science data, distilled through expert testimony. If this concern becomes paramount, we might treat "privacy" as a pure question of law, which would allow trial courts to develop a set of bright-line rules regarding the division between the public and private realms.

Having said that, one can make a strong case that juries will do better than judges in cases requiring social network analysis. Judges are constrained by precedent and a desire to develop a coherent body of law. As a result of that, they will sometimes seize upon rules developed in one context and apply them to wholly divergent contexts. The most egregious example of this in the limited privacy context is *Zieve v. Hairston*, a Georgia case handed down a few months ago.²²² In *Zieve*, the Georgia Court of Appeals considered a privacy claim brought by a man who had undergone hair replacement surgery at his local clinic. The plaintiff had agreed to let the clinic use his "before" and "after" photographs in their television advertisements, so long as those ads did not air within 500 miles of Georgia. After advertisements featuring Zieve's photograph aired in Georgia and he was recognized by a co-worker, Zieve sued for invasion of privacy.²²³ The *Zieve* court felt that following *Kubach* (another Georgia case) required it to rule for the plaintiff, since *Kubach* has embraced the notion of limited privacy. But whereas *Kubach* reached the right result under social network theory, *Zieve* almost certainly did not. After all, Georgia residents (including Zieve's acquaintances) travel out of state and watch television while traveling; Zieve presumably had out-of-state acquaintances who would recognize him in the television advertisements and communicate with Georgia residents about this highly noteworthy information ("Hey, our buddy Zieve is on TV. You'll never guess why!"). The court should have asked how many out-of-state viewers would have seen the advertisement and explored the attributes of Zieve's social network.

²²² 598 S.E.2d 25 (Ga. Ct. App. 2004).

²²³ The facts of the case suggest breach of contract as an alternative cause of action to the plaintiff's public disclosure claim. Zieve argued that the defendant had breached its contract with him. It appears that the trial court granted the defendant a directed verdict on Zieve's claim that the defendant had breached an oral contract, but submitted the question of whether the defendant had breached its written contract to the jury. *Id.* at 28. The appellate court did not consider issues relating to either breach of contract claim on appeal.

Yet the *Zieve* court did not examine any of these social network questions, slavishly applying *Kubach*'s apparent holding to an easily distinguishable case. Adherence to precedent, in this instance, caused the court to disregard the inquiries dictated by social science and commonsense.²²⁴

Indeed, adherence to precedent may be undesirable in the realm of privacy law, given the rapidity with which new technologies and new norms can cause expectations of privacy to change. Making "privacy" an issue of law threatens to ossify obsolete expectations of privacy that existed in an earlier era.²²⁵ Of course, for the same reason, courts considering social network analysis ought to be wary of relying on dated social science – a classic study like Schachter and Burdick's²²⁶ ought to be judged in light of recent developments at girls' schools, like text-messaging, blogging, and the substantial changes in adolescent culture that have occurred in the intervening years. In light of all this, we may prefer to have the law of privacy determined by responsive juries that need not worry about creating consistency in the law, provided the expert testimony at trial informs the jury about how to apply insights from social network theory. The world is a complicated place, and many of the "rules" of social network theory cannot be reduced to West headnotes.²²⁷

C. Institutional Competence

Some readers undoubtedly will lack confidence in the ability of courts to resolve the technically difficult social network analysis problems that are embedded in privacy tort cases. This concern might be particularly salient in light of the vexing problems of hindsight bias that arise in the public disclosure of private facts context.²²⁸

But let us survey the performance of courts in evaluating the reasonableness of privacy protections in leading cases. The courts in *Sanders* and *Fisher* reached intuitive conclusions that map well onto the likely results of predictive social network analysis.

²²⁴ I have found a few other cases in which the courts have stretched the notion of limited privacy too far, most notably in *Virgil v. Time, Inc.*, 527 F.2d 1122 (9th Cir. 1975); *Green v. Chicago Tribune*, 675 N.E.2d 249 (Ill. Ct. App. 1996); and *Veilleux v. Time*, 8 F. Supp.2d 23 (D. Maine 1998). In all of these cases, courts held that the subject's willingness to share information with a journalist, on the record, did not indicate a willingness to share the information with the journalist's readers. Notably, *Green* relied heavily on *Virgil*, and *Veilleux* relied on both *Virgil* and *Green*. Alabama decisions relying on *Nader* made the same mistake, but in the opposite direction, holding that one's willingness to share previously private information with friends necessarily indicated a willingness to share information with the general public. See *supra* note 72.

²²⁵ For a report on the results of national polls dealing with privacy matters, and how responses have varied over time, see James E. Katz & Annette R. Tassone, *The Polls – A Report: Public Opinion Trends: Privacy and Information Technology*, 54 PUB. OP. Q. 125 (1990).

²²⁶ See *supra* note 153.

²²⁷ Nor can they be translated into bullet points for readers of this law review article. To repeat, social network analysis is often context-dependent in ways that defy easy characterization or simplistic modeling. The "rules" of social network theory (e.g., the strength of weak ties, the tendency for social networks to be scale free, the tendency of information of information to degrade as it passes through a social network) necessarily operate at a medium to high level of generality.

²²⁸ On hindsight bias, see Christine Jolls, Cass R. Sunstein, & Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1523-31 (1998).

The court in *Kubach* reached an arguably counterintuitive result that is well-supported by social network studies of dissemination of the information at issue there. In *Nader* and *Y.G.*, hard cases both, the courts reached defensible results, though I have suggested that courts might have asked for additional factual information that should have had some bearing on the likelihood of subsequent dissemination there. Only in *Duran* were the court's intuitions about how information might spread through society far off the mark, and perhaps hindsight bias is to blame there.

In assessing this performance, courts appear to do a pretty good job of intuiting sound answers to what are essentially predictive social network analysis problems. But they provide little by way of explanation for these results, other than articulating or rejecting the notion of limited privacy. Given this background, it may well be that with a bit more methodological rigor and a few hints about experimental and empirical results – particularly in those instances where social network studies produce counterintuitive findings – courts can craft more transparent, and hence more persuasive, opinions in these kinds of cases.²²⁹

Indeed, if courts are able to gauge the risks of information dissemination with reasonable accuracy, perhaps ordinary people can too.²³⁰ One promising sociological research agenda would try to see how closely lay people's guesses about the extent of information dissemination tracks the actual data on information dissemination.²³¹ If people learn, through experience, how likely dissemination is to occur, then this should comfort those worried about the law's decision to disregard subjective expectations of privacy in torts doctrine and my advocacy of such an approach.²³² Subjective expectations of privacy and objectively reasonable expectations of privacy could correlate reasonably well. What little evidence we have on this front shows that people have a tendency to overestimate their own centrality within social networks.²³³ This

²²⁹ Slobogin & Schumacher are less positive in their assessment of the Supreme Court's Fourth Amendment jurisprudence, as they note several instances in which the Court's reasonable expectations of privacy differ substantially from survey respondents. Slobogin & Schumacher, *supra* note 35, at 740-42. This is interesting, since the Court has eschewed formal survey data in the Fourth Amendment context, just as the courts have ignored social network analysis in the privacy tort setting.

²³⁰ Or maybe not. Obvious differences include judges' access to the fruits of the discovery process and the adversarial system of justice. Judicial detachment may also help them see social networks more accurately than people who are embedded in them. Indeed, social networks research suggests that individuals tend to overstate their own importance in a particular social network and overestimate the degree of connectedness among their own friends. See Kumbasar et al., *supra* note 106, at 499.

²³¹ As best I can tell, however, no one in sociology is pursuing such an agenda. The closest related research agenda appears to be that of Tiziana Casciaro, at the Harvard Business School. Casciaro is studying individuals' perceptions of the social networks that surround them. She has found that location within a social network, and personality traits such as positive affect substantially affect the accuracy of people's perceptions. See Tiziana Casciaro et al., *Positive Affectivity and Accuracy in Social Network Perception*, 23 MOTIVATION & EMOTION 285 (1999); Tiziana Casciaro, *Seeing Things Clearly: Social Structure, Personality, and Accuracy in Social Network Perception*, 20 SOCIAL NETWORKS 331 (1998).

²³² We do know that people differ in their ability to accurately map the information flow through their own social networks. See *supra* note 231; Bondonio, *supra* note 91, at 325-26; Casciaro et al., *supra* note 231, at 292. We might suppose on the basis of this data that peoples' ability to intuit social network theory insight vary as well.

²³³ See *supra* note 230.

suggests, in turn, that an individual will have a tendency to overestimate the extent to which his acquaintances will find the details of his private life worth discussing. If courts apply an objective measure of reasonable privacy expectations, they will probably err on the side of protecting privacy too little, rather than too much.²³⁴ Judicial errors of the *Duran* variety will be more common than judicial errors of the *Zieve* variety.

We may also expect that helpful feedback mechanisms will develop from courts' occasional use of sociological research in the same way that economic research is occasionally used at present by courts. Although I have found a few illuminating studies, the dissemination of previously private information through social networks has not been a central concern of sociologists. Yet the privacy context seems like the most obvious application of this discipline to a field of law. Were courts to take social networking seriously, one can imagine that sociologists will conduct more studies like the HIV disclosure and bakery rumor studies, each of which teaches a great deal about the dissemination of previously private information through particular social networks.

D. *Extensions of the Approach*

The issue of reasonable expectations of privacy or confidentiality cuts through many different substantive fields of law, including Fourth Amendment law,²³⁵ the constitutional right of information privacy,²³⁶ Freedom of Information Act privacy,²³⁷

²³⁴ By "too little" I mean, relative to the parties' actual subjective expectations of privacy.

²³⁵ See, e.g., *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *United States v. Miller*, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *Contra Smith*, 442 U.S. at 748, 749 (Marshall, J., dissenting) ("[E]ven assuming . . . that individuals 'typically know' that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.") (footnote omitted); *Burrows v. Superior Court*, 529 P.2d 590 (Cal. 1974) (embracing a notion of limited privacy, with respect to bank records, under the California Constitution).

Kyllo v. United States, 533 U.S. 27 (2001), seems somewhat receptive to the probabilistic approach that I have advocated herein. In *Kyllo* the Court held that using sense-enhancing technology to obtain information about the interior of a home is a search for Fourth Amendment purposes, "at least where . . . the technology in question is not in general public use." *Id.* at 34. This "general public use" language suggests that, to some degree, obscurity is privacy, and people have a reasonable expectation of privacy against facts that an individual might conceivably, but probably won't, discover about them.

²³⁶ See generally *Whalen v. Roe*, 429 U.S. 589 (1977) (holding that the disclosure of information about who has used prescription medication to New York law enforcement officials did not violate the plaintiffs' constitutional right to information privacy, since such information was already routinely shared with health care providers and insurance industry employees); *Doe v. Borough of Barrington*, 729 F.Supp. 376 (D.N.J. 1990) (recognizing a constitutional right of information privacy claim where an individual disclosed his HIV status to police officers in order to prevent them from coming into contact with his open skin sores, and the officers later disclosed the man's HIV status to his neighbors).

various evidentiary privileges,²³⁸ patents,²³⁹ and trade secrets law.²⁴⁰ In this paper, I have for the most part confined my analysis to the privacy torts context. There are a couple of reasons for this. First, the notion of limited privacy has found receptive audiences in the torts cases, and so incorporating ideas from social network theory into the law would not require wholesale revision of the tort laws in many states. Second, and relatedly, a notion of limited privacy might be more normatively appealing in the tort context than in some other contexts.²⁴¹ That said, there may be substantial benefits from unifying these divergent bodies of privacy law, and, in the event that the current paper persuades some of its readers, future work will explore applications of network theory to some or all of these fields.

Beyond the potential for insights about these substantive fields, the study of social networks opens up enormous possibilities for those who fancy themselves scholars of the law and social norms. First generation social norms scholarship suggested that gossip networks could be highly effective in facilitating informal social control, as an alternative to formal law.²⁴² In recent years, the social norms literature may have lost a little bit of momentum. One way for legal scholars to recover that momentum is to study gossip networks in more rigorous ways, so that we can evaluate when informal social control might function as a welfare-enhancing alternative to legal process.

This idea has many potential applications, but two examples here will be illustrative: If we learn that gossip networks in the landlord-tenant context are highly efficient, the law ought to be more receptive to landlord self help.²⁴³ Similarly,

²³⁷ See, e.g., *United States Department of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749 (1989) (holding that an FBI rap sheet was private within the meaning of the Freedom of Information Act's 7(c) privacy exception).

²³⁸ E.g., *United States v. Evans*, 113 F.3d 1457, 1462 (7th Cir. 1997) ("Thus as a general matter, the attorney-client privilege will not shield from disclosure statements made by a client to his or her attorney in the presence of a third party who is not an agent of either the client or attorney.")

²³⁹ See, e.g., *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1548 (Fed. Cir. 1983) (defining "secret" prior use); *Rosaire v. National Lead Co.*, 218 F.2d 72 (5th Cir. 1955) (holding that a quite obscure prior use deprived a subsequent inventor of novelty).

²⁴⁰ *Rockwell Graphic Sys. v. DEV Indus.*, 925 F.2d 174 (7th Cir. 1991) (holding that while the plaintiff "could have done more" to protect the confidentiality of its trade secrets, "perfect security is not optimum security," and so the plaintiff was entitled to a jury trial on misappropriation of trade secrets despite having shared the secret with numerous vendors); *Wilkes v. Pioneer Am. Ins. Co.*, 383 F. Supp. 1135, 1141 (D.S.C. 1974) (holding that absolute secrecy is not required in order for a trade secret to be protected, but a "substantial element of secrecy must exist").

²⁴¹ A criminal defendant might say that he was perfectly willing to share information about a criminal conspiracy with his co-conspirators, but had a reasonable expectation that the information would not be disseminated outside the group of co-conspirators. When the communication at issue concerns violations of criminal laws, there may be strong justifications for holding that lessened expectations of privacy attach or deeming such expectations altogether irrelevant. Cf. discussion of *Fisher*, *supra* text accompanying note 218.

²⁴² See *supra* note 22 and accompanying text.

²⁴³ The idea here is that landlords who lock out tenants improperly will be sanctioned by the marketplace if gossip functions well. Would-be tenants would pay a premium to rent from landlords who have a reputation for behaving reasonably. If, on the other hand, tenant gossip networks function poorly, then the fear of a market sanction may inadequately deter landlords from engaging in opportunistic or illegal

inefficiencies in the social networks of lawyers and legal clients may explain the need for judges to impose Rule 11 sanctions against litigators who misbehave.²⁴⁴ Understanding the relevant social networks helps us evaluate the need for legal regulation of private actors. Social network theory, in short, may lay the foundation for a second generation of interesting social norms scholarship.

V. Conclusion

Privacy torts doctrine directs judges to evaluate whether it was appropriate for a plaintiff to assume that her initial disclosure of information about herself would result in the widespread dissemination of that information. As most courts understand this test, it calls for seemingly difficult, generally counterfactual, ex ante analysis that sociologists are better equipped to perform. In light of all this, it is perhaps surprising that courts seem to reach defensible results in many of the leading privacy cases. Their analysis leaves something to be desired, and I have tried to show that insights from social network theory can improve that analysis. The substantial recent improvements in the quality of this body of social science, mediated through expert testimony, ought to find their way into American courtrooms.

The paper that I have written attempts to furnish courts with a theory of privacy that they can embrace readily, taking as a given the choice of these courts to base the privacy determination on what the parties should have expected to follow the initial disclosure of information by someone other than the defendant. Where a defendant's disclosure materially alters the flow of otherwise obscure information through a social network, such that what would have otherwise remained obscure becomes widely known, the defendant should be liable for public disclosure of private facts. By the same token, when a court must determine whether a defendant has intruded upon the plaintiff's seclusion by improperly gathering information about the plaintiff's private matters or affairs, judges ought to ask whether the plaintiff's information was likely to have remained obscure had the defendant never acted. For both these torts, social network theory holds out the promise of replacing the common law's vagueness with a relatively objective, testable, rigorous, and principled approach.

behavior. For recent efforts to enhance the efficiency of the tenant gossip network, see <<http://www.apartmentratings.com>>, and <<http://apartmentreviews.net>>. For more on landlord self help, see *Berg v. Wiley*, 264 N.W.2d 145 (Minn. 1978).

²⁴⁴ With a perfectly efficient social network, judicial scoldings of attorneys in open court, combined with observations of misconduct by opposing counsel, would deter adequately those attorneys who hoped to win clients in the future.