THE CASE FOR ONLINE OBSCURITY

Woodrow Hartzog[*] *and Frederic Stutzman*[**]

ABSTRACT: On the Internet, obscure information has a minimal risk of being discovered or understood by unintended recipients. Empirical research demonstrates that Internet users rely on obscurity perhaps more than anything else to protect their privacy. Yet, online obscurity has been largely ignored by courts and lawmakers. In this article, we argue that obscurity is a critical component of online privacy, but it has not been embraced by courts and lawmakers because it has never been adequately defined or conceptualized. This lack of definition has resulted in the concept of online obscurity being too insubstantial to serve as a helpful guide in privacy disputes. In its place, courts and lawmakers have generally found that the unfettered ability of any hypothetical individual to find and access information on the Internet renders that information public, or ineligible for privacy protection. Drawing from multiple disciplines, this article develops a focused, clear, and workable definition of online obscurity: Information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We have identified four of these factors: 1) search visibility, 2) unprotected access, 3) identification, and 4) clarity. This framework could be applied as an analytical tool or as part of an obligation. Obscurity could be relied upon as a continuum to help determine if information is eligible for privacy protections. Obscurity could be used as a protective remedy by courts and lawmakers; instead of forcing websites to remove sensitive information, a compromise could be some form of mandated obscurity. Finally, obscurity could serve as part of an agreement. Internet users bound to a "duty to maintain obscurity" would be allowed to further disclose information, so long as they kept the information generally as obscure as they received it.

[*] Assistant Professor of Law, Cumberland School of Law at Samford University; Affiliate Scholar, Center for Internet and Society at Stanford Law School.
[**] Postdoctoral Fellow, H. John Heinz III College, Carnegie Mellon University.

CONTENTS

INTRODUCTION

Internet users routinely hide information by making it invisible to search engines, using pseudonyms and multiple profiles, and taking advantage of privacy settings. Individuals rely on the obscurity created by these techniques to protect their privacy perhaps more than anything else.[1]

[1] *See, e.g.,* danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life, in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 133 (David Buckingham ed., 2008), http://www.mitpressjournals.org/doi/pdf/10.1162/dmal.9780262524834.119 ("Most people believe that security through obscurity will serve as a functional barrier online. For the most part, this is a reasonable assumption."); James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009); Danielle Citron, *Fulfilling Government 2.0's Promise With Robust Privacy Protections,* 78 GEO. WASH. L. REV. 822, 835 (2010) ("People also have a sense that their social-network information will be kept private because they feel anonymous amidst the millions of social-network users."); Lauren Gelman, *Privacy, Free*

Yet, incredibly, the concept of obscurity has languished in legal privacy doctrine. Courts have attempted to refine other complex privacy concepts such as "publicity,"[2] "newsworthy,"[3] a "reasonable expectation of privacy,"[4] and others. However, obscurity is generally equated with "hidden" and then dismissed as an unhelpful concept in privacy disputes. Or, obscurity is conflated with other concepts such as confidentiality or the notion of "public information" and consequently overlooked as a distinct concept that could aid in the analysis of privacy disputes. The neglected and distorted state of obscurity in privacy doctrine is a significant problem because the concept of obscurity is too central to the expectations of Internet users for courts and lawmakers to ignore.

This article has three main purposes: 1) To demonstrate that obscurity is a crucial component of online privacy that has largely been ignored by the law; 2) To conceptualize online obscurity in a useful way for privacy doctrine; and 3) To propose ways that our conceptualization could be implemented to remedy the tension between privacy law and Internet users' experience and expectations. By defining online obscurity, this article aims to provide a framework that is more effective than the current approach in answering some of the difficult legal questions regarding online privacy.

The importance of obscurity has dramatically increased since the advent of the social Web. The original one-way broadcast nature of the Web has given way to a virtually endless patchwork of private conversations, back alleys, hidden forums and walled gardens. It has been estimated that 80-99 percent of the World Wide Web is completely hidden from general-purpose search engines and only accessible by those with the right search terms, URL, or insider knowledge.[5] Other pieces of online information are

Speech and Blurry-Edged Social Networks, 50 B.C. L. REV. 1315 (2009). This assertion is addressed in greater detail in Section II.

[2] *See, e.g.*, Miller v. Motorola, Inc., 560 N.E.2d 900 (Ill. Ct. App. 1990); Yoder v Smith, 112 N.W.2d 862 (Iowa 1962); Brents v. Morgan, 299 S.W. 967 (Ky. 1927); Beaumont v. Brown, 257 N.W.2d 522 (Mich. 1977).

[3] *See, e.g.*, Sipple v. Chronicle Publ'g Co., 201 Ca. Rptr. 665 (Cal. Ct. App. 1984); Virgil v. Time, 527 F.2d 1122 (9th Cir. 1975); Neff v. Time, Inc., 406 F. Supp. 858 (W.D. Pa. 1976).

[4] *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967); Smith v. Maryland, 442 U.S. 735 (1979); Illinois v. Caballes, 543 U.S. 405 (2005).

[5] *See, e.g.*, Michael Bergman, *The Deep Web: Surfacing Hidden Value*, 7 JOUR. OF ELEC. PUBL'G, at http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104 (2001) ("Since they are missing the deep Web when they use such search engines, Internet searchers are therefore searching only 0.03% — or one in 3,000 — of the pages available to them today."); Andy Beckett, *The Dark Site of the Internet*, THE GUARDIAN (Nov. 26, 2009), http://www.guardian.co.uk/technology/2009/nov/26/dark-side-internet-freenet; Russell

obfuscated by the use of pseudonyms, multiple profiles, and privacy settings. Is this functionally obscure information any different in practice than information protected by a password? The law is inconsistent in its answer, and this is a problem.

Because courts and lawmakers have failed to develop online obscurity as a concept, the law in a number of online privacy disputes remains difficult to square with the expectations of Internet users. For example, if a blogger limits access to her website to those who have a password, are her posts considered public or private? How should courts classify pseudonymous postings that are invisible to search engines but could have been accessed by anyone in possession of the URL? If a website introduces facial recognition technology and a search option, have they broken any promises of privacy to users who previously uploaded photos and may have relied on the fact those photos were not searchable?

Drawing from empirical research from multiple disciplines, this article develops a focused, clear, and workable definition of online obscurity: Information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We have identified four of these factors as part of a non-exhaustive and flexible list: 1) search visibility, 2) unprotected access, 3) identification, and 4) clarity.

This framework could be applied to online privacy disputes in various ways. Obscurity could be used as a continuum when courts are asked to determine if information was eligible for privacy protections. Obscurity could be used as a benefit or protection – instead of forcing websites to remove information, courts and lawmakers could, in appropriate contexts, mandate a form of obscurity or embrace obscurity as a valid consumer protection technique. Finally, obscurity could serve as a metric for the boundary of allowable disclosure online as part of an agreement. It could replace confidentiality as a term in some contracts. Internet users

Kay, *Deep Web*, COMPUTERWORLD (Dec. 15, 2005), http://www.computerworld.com/s/article/107097/Deep_Web ("[M]ore than 500 times as much information as traditional search engines "know about" is available in the deep Web."); Danny Devriendt*, Data is Gold – 91,000 Terabytes of Uncharted Web: Welcome to the Dark Side*, PORTER NOVELLI BLOG (Apr. 4, 2011), http://blog.porternovelli.com/2011/04/11/data-is-gold-%E2%80%93-91000-terabytes-of-uncharted-web-welcome-to-the-dark-side/ ("The dark Web, or hidden Web is approximately 550 times bigger than the Web you experience daily."); Norm Medeiros, *Reap What You Sow: Harvesting the Deep Web*, 18 OCLC SYS. & SERV. 18 (2002); Yanbo Ru & Ellis Horowitz, *Indexing the Invisible Web: A Survey*, 29 ONLINE INFO. REV. 249 (2005) ; *see also* CHRIS SHERMAN & GARY PRICE, THE INVISIBLE WEB: UNCOVERING INFORMATION SOURCES SEARCH ENGINES CAN'T SEE (2001); PAUL PEDLEY, THE INVISIBLE WEB: SEARCHING THE HIDDEN PARTS OF THE INTERNET (2001).

bound to a "duty to maintain obscurity" would be allowed to further disclose information online, so long as they kept the information generally as obscure as they received it.

Part I of this article explores the general concept of obscurity and the vital role it plays in our everyday lives. Part II of this article focuses on online obscurity, identifying the tactics and strategies individuals employ to find obscurity in online settings. Part III of this article discusses the law's failure to embrace or develop the concept of online obscurity. Part IV introduces the proposed definition and framework for online obscurity. Finally, Part V details the ways obscurity could ameliorate some of the tension between current privacy doctrine and the expectations of Internet users.

I. THE CONCEPT OF OBSCURITY

Obscurity is a simple concept, reflecting a state of unknowing. But what does it mean for an individual to be obscure? Obscurity at the individual level involves two parties: the individual and the observer. For an individual to be obscure, her or his observers must be not know about critical information relevant to the individual that is needed to make sense *of* the individual: the personal identity, social connections, or context are examples. Without this critical information, the observers are limited in their ability to make sense of the actions and utterances of the individual. For example, if an individual gossips in the presence of the observer, the gossip is generally obscure unless the observer knows of whom the individual speaks. Obscurity is, in many ways, a commonplace and necessary social condition that facilitates interaction. In everyday interaction, we are often practically obscure in the eyes of observers. A significant portion of our everyday interaction places us into a zone of obscurity, where our identity and personal context are unknown to those we interact with or share common space.

Being obscure in the eyes of others does not mean we are unidentifiable. It is important to differentiate obscurity from anonymity. Identity and identification work at many levels; psychologists and sociologists have described identities that interact and overlap: our personal and social identities, for example.[6] More than identification, obscurity requires comprehension; therefore, the tools an observer needs to comprehend are different from those needed to identify. One may be able to make a reasonable estimation of our identity by observing our manner or dress, but our actions or conversation may remain obscure to the observer

[6] *See, e.g.*, RICHARD JENKINS, SOCIAL IDENTITY (1996).

unless critical contextual information can be deduced.[7] We have a reasonable expectation of obscurity because it is unlikely that the observation of our person would lead to the deduction of all relevant bits of information necessary to comprehend our actions or utterances. Without an observer being able to deduce and identify all relevant bits of information necessary for comprehension, we can safely interact in a zone of obscurity. In a zone of obscurity, our actions are protected not just by our lack of identification. The zone of obscurity is "fault-tolerant," in the sense that an observer that is able to identify our persons may still not be able to comprehend our action or utterances.

We argue the case for obscurity for two reasons. First, we argue that being in a zone of obscurity is commonplace, and therefore our expectation of obscurity will transfer to the domains in which we spend time, both physical and virtual. Second, we argue that obscurity is a meaningful state where we are protected by an observer's inability to comprehend our action, and therefore social practice encourages the seeking of obscurity. In the following section, we explore the cognitive and cultural logic of obscurity, focusing particularly on Dunbar's analysis of cognitive economy and how it produces obscurity, and Goffman's analysis of interaction – particularly, how we enact obscurity in everyday life. While obscurity is a fundamentally natural and common state, we feel that the concept of obscurity is both under-theorized and poorly identified. By contributing an analysis of individual experience of obscurity, we argue that obscurity is both a physically essential state and one that is culturally and normatively recognized. By making these simple points, we will then be able to extend our analysis of the logic of obscurity to online settings, where obscurity is equally commonplace.

In arguing that obscurity is commonplace, we draw on the work of evolutionary biologist Robin Dunbar to illustrate the cognitive logic of obscurity. Dunbar's work on the "Social Brain Hypothesis" famously demonstrated that human cognitive groups are fairly small, with a maximum group size of approximately 150 members. According to Dunbar, a cognitive group is a group of individuals that have shared communication, memories and dyadic relationships within the group. Put another way, within human groups, the maximum size of a group than an individual can make sense of at the individual level is 150.[8] Dunbar was

[7] Michael A. Hogg, Deborah J. Terry, & Katherine M. White, *A Tale of Two Theories: A Critical Comparison of Identity Theory with Social Identity Theory*, 58(4) SOC. PSYCHOL. Q. 255 (1995).

[8] *See e.g.*, Robin I.M. Dunbar, *Co-Evolution of Neocortex Size, Group Size and Language in Humans*, 16(4) BEHAV. AND BRAIN SCI., 681 (1993); Robin I.M. Dunbar & Matt Spoors, *Social Networks, Support Cliques, and Kinship*, 6(3) HUM. NATURE 273 (1995).

careful to draw a distinction between simple identification and true knowing, pointing out that we can recognize about 2,000 people, a much larger number than the maximum cognitive group size.[9] The social brain hypothesis illustrates the evolutionary logic to a cognitive economy of obscurity: to prevent the overburdening of memory, our cognitive groups are kept manageable, which means that most interactions outside cognitive groups occur in zones of obscurity. Viktor Mayer-Schonberger, in his work on digital memory *Delete: The Virtue of Forgetting in the Digital Age*, has extended this logic, highlighting work that demonstrates that forgetting is a cognitive advantage.[10] Our memories are purposefully selective to prevent cognitive overburdening. This realistically means that most of the individuals we interact with in passing, or share common space in transit, are obscure to us and we to them – they are strangers. Furthermore, the nature of obscurity in interaction with strangers produces notable effects, such as conversational freedom.[11] Most of us live a day-to-day existence where we are only non-obscure (obvious), to a few close individuals.[12] This is partially due to an important cognitive orientation towards selective memory that produces obscurity. Genetic disposition towards obscurity is therefore reinforced by everyday practice.

It is important refrain from conflating the lack of personal identification with anonymity. In everyday life others identify us at varying personal and social levels.[13] We are identified to others through appearance, our role or position, or through ritual activity. For example, we are able to construct a set of expectations of a man wearing a Roman collar without knowing his personal identity. We also come to know those we interact with regularly but do not identify personally, such as the neighbor who walks her dog at a certain time every day, or the barista that serves morning coffee. These abstract identifications can lead to personal identifications within groups, particularly in cases where the behavior deviates from norm or expectation.[14] Indeed, the potential of identification

[9] Robin I.M. Dunbar, *The Social Brain Hypothesis*, 6(5) EVOLUTIONARY ANTHROPOLOGY: ISSUES, NEWS, AND REVIEWS 178 (1998).

[10] VIKTOR MAYER-SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2010).

[11] John A. Bargh, Kaetlyn Y.A. McKenna, & Grainne M. Fitzsimons, *Can You See the Real Me? Activation and Expression of the "True Self" on the Internet*, 58(1) JOUR. OF SOC. ISSUES 33 (2002).

[12] The notable exception being celebrities or other highly identifiable individuals. *See also* GRAEME TURNER, UNDERSTANDING CELEBRITY (2004).

[13] SUSAN A. FISKE & SHELLY E. TAYLOR, SOCIAL COGNITION (2nd ed. 1991); John M. Levine, Lauren B. Resnick, & Tory E. Higgins, *Social Foundations of Cognition*, 44(1) ANN. REV. IN PSYCHOL. 585 (1993).

[14] In offline settings, we can imagine deviant behavior generating information needs that use personal identification as part of the explanatory framework. For example, finding out

serves as a strong structural role in fostering normative behavior, as anyone who has been exhorted to behave a certain way because "you never know who is watching." Therefore, humans employ a range of strategies to produce obscurity, to increase the odds that their actions or bodies can not be fully comprehended (in some cases) or identified (in others). Thus, it is important to explore how obscurity is produced in everyday life.

As the sociologist Erving Goffman argues, processes of identification and comprehension are a function of the range of signals we give off both purposefully and accidentally. Our dress and demeanor convey "front-stage" signals – those we intend our observers to draw upon as they make sense of our actions. Of course, we also give off subconscious or accidental signals: it is often these "back-stage" signals that truly enable observers to make sense of what they are observing.[15] For example, an individual effectuating a certain dialect may momentarily slip up, revealing information about one's social class or background unintentionally. According to Goffman, our ability to "read" a scene, and thus appropriately judge how we present ourselves, is a critical component in social interaction.[16] In his book *Behavior in Public Places*, Goffman describes how we utilize a range of cues and physical structures to figure out how we should present ourselves.[17] For example, our understanding of the private nature of a conversation is moderated by the presence of walls and doors – physical structures that provide privacy and feature into the structure and content of interpersonal interaction. We might say things behind a closed door that we would not say in public.

Following Goffman's logic, we argue that individuals both consciously and subconsciously attempt to "produce" obscurity to protect their persons (defensively) or advance their goals (offensively). An individual effectuating a certain type of accent may actually be using obscurity offensively, to create an unrealistic impression, whereas another individual may cloak him or herself in obscurity to prevent informational

the back-story for why an unidentified neighbor did something rude. In online settings, the role of deviant behavior has been shown to interact with group membership status. *See* Zuoming Wang, Joseph B. Walther & Jeffrey T. Hancock, *Social Identification and Interpersonal Communication in Computer-Mediated Communication: What You Do Versus Who You Are in Virtual Groups*, 35(1) HUMAN COMM. RES. 59 (2009).

[15] ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

[16] Of this particular challenge, Goffman writes "Whatever else, our activity must be addressed to the other's mind, that is, to the other's capacity to read our words and actions for evidence of our feelings, thoughts, and intent. This confines what we say and do, but it also allows us to bring to bear all of the world to which the other can catch allusions." Ergin Goffman, *Felicity's Condition*, 89(1) AM. JOUR. OF SOC., 1 (1983).

[17] ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES: NOTES ON THE SOCIAL ORGANIZATION OF GATHERINGS (1966).

leakages. In both cases, the individual "performs" an identity and draws upon cues from the audience of observers to construct an optimized zone of obscurity.[18]

The anthropological and sociological theories of Dunbar and Goffman lend nuance to how we understand personal obscurity. Dunbar's notion of small cognitive groups provides evidence that obscurity is a self-reinforcing phenomena, and obscurity is closely tied to our geographies and patterns of interaction. Goffman also highlights the self-reinforcing nature of obscurity: our presentations are a function of our audience, and a key component of interpersonal interaction is managing one's audience. This management can occur by simply "playing the part" in everyday interaction, or employing physical barriers as privacy protections. These deeply ingrained tactics of identity protection and performance control have long served and self-reinforced our notions of obscurity. The next section considers how our expectations of obscurity offline impact our privacy decisions online, and how the practice of obscurity is enacted online, where geography, identity presentation, and physical structure are very different.

II. EMPIRICAL SUPPORT FOR ONLINE OBSCURITY

When an individual decides to share information online, her or his actions are shaped by implicit and explicit rules, cultural norms, prior attitudes, expectations, and desired outcomes.[19] Much as in everyday life, the choice to disclose online is the product of a complex and highly contextual decision process, where risks are weighed against the potential reward of disclosure. It is normal to expect obscurity in everyday life, and obscurity is the self-reinforced product of physical, social, and cognitive processes. Because obscurity is a normative state, we argue that obscurity is expected, and actively produced, in online settings. Although early research on Internet users focused on individual differences between users and the general population, Internet use is now so widespread that differences between users and non-users are largely attributable to socio-economic or

[18] The notion of a zone of obscurity being optimized is in line with the work of Altman and Petronio, who both argue that privacy is regulated recursively and interactively with others. *See* SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE (2002); IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975).

[19] See *e.g.* ADAM N. JOINSON, & CARINA B. PAINE, SELF-DISCLOSURE, PRIVACY AND THE INTERNET. OXFORD HANDBOOK OF INTERNET PSYCHOLOGY 237 (2007); Rob Kling, Ya-Ching Lee, Al Teich & Mark S. Frankel, *Assessing Anonymous Communication on the Internet: Policy deliberations*, 15(2) THE INFO. SOC'Y. 79 (1999); Su-Yu Zeng, Ling-Ling Wu & Houn-Gee Chen, *Sharing Private Information Online: The Mediator Effect of Social Exchange*, In Proceedings of the 11th International Conference on Electronic Commerce, New York, NY, USA, 231 (2009).

geographic differences, and not behavioral or attitudinal differences.[20] Therefore, we believe that online obscurity is generally expected, and not the sole purview of a certain class of Internet user.

What does it mean to expect obscurity online? We propose a non-exhaustive, illustrative list of these expectations. First, individual use of the Internet does not necessarily indicate the seeking of a wide audience, or at least an audience wider than offline expectations. A user of the Internet does not expect fame or notoriety simply because they use the Internet, nor does this Internet user inherently seek fame or notoriety. Multiple studies of attention and audience online have revealed a "long tail" or pareto distribution of attention online, which means that the majority of attention online is dedicated to a small number of producers, with the majority of content producers having small audiences.[21] Second, individual use of the Internet is influenced by, and reflective of, existing cognitive schema. That is, our identities, expectations, roles and norms will often transfer to online settings. While the Internet theoretically affords the opportunity for individuals to "be anyone," in the age of ubiquitous social media it is more likely that Internet use will simply reinforce our offline social structures.[22] For example, in Dennen's field study of academic bloggers, six elements of online identity were identified, including name, profile, content, voice, affiliation, and design/presentation, all of which have strong offline

[20] *See, e.g.*, Susannah Fox, *Digital Divisions: There Are Clear Differences among Those with Broadband Connections, Dial-up Connections, and No Connections at All to the Internet*, PEW INTERNET & AMERICAN LIFE PROJECT (Oct. 5, 2005), http://www.pewinternet.org/PPF/r/165/report_display.asp; John B. Horrigan, *Home Broadband Adoption 2009*, PEW INTERNET & AMERICAN LIFE PROJECT (June 17, 2009). http://www.pewinternet.org/Reports/2009/10-Home-Broadband-Adoption-2009.aspx. As these reports clearly indicate, use and non-use of Internet resources is largely a function of socio-economic and geographic factors. While it is likely that a certain portion of the population opts-out of the Internet for privacy-related reasons, the proportion of individuals for whom this applies is so small it does not appear on nationally representative studies.

[21] *See, e.g.*, Jon Kleinberg, *Authoritative Sources in a Hyperlinked Environment*, 46(5) JOUR. OF THE ACM 604 (1999); Andrei Broder, Ravi Kumar, Maghoul Farzin, Prabhakar Raghavan, Sridhar Rajagopalan, Raymie Stata, Andrew Tomkins, & Janet Wiener, Graph Structure in the Web, 33 COMPUTER NETWORKS 309 (2000). For an applied discussion of attention networks in Twitter, *see* Meeyoung Cha, Hamed Haddadi, Fabricio Benevenuto, & Krishna P.Gummadi, *Measuring User Influence in Twitter: The Million Follower Fallacy*, Proceedings of the 4th International Conference on Weblogs and Social Media (2010).

[22] *See* Robert E. Kraut, Sara B. Kiesler, Bonka S. Boneva, Jonathon N. Cummings, Vicki Helgeson, & Anne Crawford, *Internet Paradox Revisited*, 58(1) JOUR. OF SOC. ISSUES 49 (2002)(discussing how selection effects confound the analysis of differences between early Internet users and non-users.).

identification analogues.[23] Academic bloggers that wished to protect their identity would use pseudonyms and other methods of identity obfuscation. This model of identity protection strongly parallels offline models of withdrawal, where identification and access is granted to a selected few.[24]

While cognitive models of online participation are strongly influenced by our offline models, there are important differences. Kling and colleagues' discussed two major structural differences in online and offline communication in their analysis of online anonymity.[25] First, online discussion is amenable to "mass dissemination," as messages posted online have the capacity to be transmitted much faster than through traditional or word of mouth campaigns. Second, messages posted online have "persistence," such that messages can be replicated, archived, and essentially made permanent through cheap digital copies. Writing in 2008, social media scholar danah boyd made a similar argument, in which she described the four primary components of networked publics, or digital public spheres for socio-technical interaction.[26] The components are: persistence, searchability, replicability, and invisible audiences. The core logic of boyd's persistence and replicability components mirror the work of Kling and colleagues' discussion of persistence and mass dissemination, so they are not discussed at length. Searchability, according to boyd, is a property of networked publics that describes the ability of third parties to quickly and efficiently "search" a public, through a keyword search or other common information retrieval function. There is no parallel in offline space, boyd argues, no universal mechanism that allows instantaneous searching through all possible geographies. Invisible audiences refers to the state of unknowing that is common in online disclosure; when sharing a post or tweet online, we have a general idea who sees our content, but we do not actually know the complete audience. Compare this to the offline equivalent; when we disclose in public, we generally have an idea of our audience, even if we do not know our audience. Because disclosures online

[23] Virginia Dennen, *Constructing Academic Alter-egos: Identity Issues in a Blog-based Community*, 2(1) IDENTITY IN THE INFO. SOC'Y 23 (2009).

[24] *See, e.g.*, SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE (2002); IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975).

[25] Rob Kling, Ya-Ching Lee, Al Teich & Mark S. Frankel, *Assessing Anonymous Communication on the Internet: Policy deliberations*, 15(2) THE INFO. SOC'Y. 79 (1999).

[26] danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life, in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 133 (David Buckingham ed., 2008), http://www.mitpressjournals.org/doi/pdf/10.1162/dmal.9780262524834.119.

are persistent and amenable to simple recontextualization, we are unable to predict the breadth of our disclosure over time.[27]

The challenge faced by users of Internet technologies, and particularly social technologies, when managing personal disclosure online, is the normative requirement to act within socially constructed rules of interpersonal disclosure, which draw strongly on offline norms, while also managing privacy and disclosure goals in light of key structural differences in the environment, such as those defined by Kling and boyd. In the following section, we explore the practice of online obscurity. We demonstrate that obscurity is both expected and sought online, and that obscurity is an increasingly important and pervasive technique for managing individual disclosure online.

A. Finding Obscurity in Nonymous Environments

In recent years, the development and adoption of technologies that enable the peer production of Internet content[28] have resulted in dramatic increases in online participation and sharing.[29] According to the Pew Internet and American Life project, nearly 75% of all adults use the Internet, and virtually all teens 12-17 (93%) are Internet users. While the broad-based growth and adoption of Internet technologies is a remarkable story, the changing nature of Internet use is equally remarkable. The explosion in peer-produced content, particularly social network sites and microblogs, has led to the production of a large amount of identity-centric ("nonymous") content – where individuals are both the producers and consumers of content *about themselves*. This shift is dramatic, and has serious implications for both privacy and identity online. Zhao and

[27] As an example, we may wish to consider the case of Aleksy Vayner, whose video resume "Impossible is Nothing" became an Internet meme. *See* DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR AND PRIVACY ON THE INTERNET 171-178 (2007).

[28] *See, e.g.,* BLOGGER (May 3, 2011), http://www.blogger.com/, WORDPRESS (May 3, 2011), http://wordpress.com/, TWITTER (May 3, 2011), https://twitter.com/, FACEBOOK (May 3, 2011), https://www.facebook.com/, FOURSQUARE (May 3, 2011), https://foursquare.com/.

[29] *See e.g.* Amanda Lenhart & Mary Madden, *Teens, Privacy and Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of Myspace*, PEW INTERNET & AMERICAN LIFE PROJECT (Apr. 18, 2007), http://www.pewinternet.org/PPF/r/211/report_display.asp; Amanda Lenhart, *Adults and Social Network Websites*, PEW INTERNET & AMERICAN LIFE PROJECT (Jan. 14, 2009), http://www.pewinternet.org/PPF/r/272/report_display.asp.; Amanda Lenhart, Kristen Purcell, Aaron Smith & Kathryn Zickuhr, *Social Media and Young Adults*, PEW INTERNET & AMERICAN LIFE PROJECT (February 3, 2010), http://pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

colleagues characterize the implications of "nonymous technologies," and the challenges for researchers and scholars:

> Identity construction in a nonymous online environment has not been well studied. Unlike the anonymous setting in which individuals feel free to be whatever they want to, the nonymous environment places constraints on the freedom of identity claims. A faculty member on his or her departmental listserv, for example, cannot claim to be someone else without prompting an immediate inquiry. This certainly does not suggest that there will be no self-presentation in nonymous online environments. Identity performance takes place even in places where individuals are fully identifiable, such as in classrooms and offices, but self-performances in such contexts are constrained and tend to conform to established social norms. Depending on the degrees of nonymity in the given situation, the level of conformity varies accordingly.[30]

As Zhao and colleagues note, the shift from anonymous to nonymous communication in online settings pose a number of challenges. First, nonymous communication online is not well studied; scholarship on computer-mediated communication has, until recently, heavily focused on the challenges and opportunities of anonymous communication settings. Second, Zhao and colleagues describe the relatively novel overlap between nonymous mediated communication settings and offline settings. That is, with the growth of peer-produced content, we are increasingly communicating nonymously online with those we interact with offline.[31] Therefore, privacy management in nonymous online communication requires the management of overlaps and boundaries in offline networks – if one wishes to communicate nonymously yet maintain control over disclosures, he or she must develop strategies that permit selective or targeted disclosures. In this section we review literature that identifies some of these techniques of managed disclosure. In doing so, we demonstrate that the practice of obscurity is a useful concept in both nonymous and anonymous environments.

[30] Shanyang Zhao, Sherri Grasmuck, & Jason Martin, *Identity Construction on Facebook: Digital Empowerment in Anchored Relationships*, 24(5) COMPUTERS IN HUMAN BEHAVIOR, 1816, 1818-1819 (2008)(citations omitted).

[31] Cliff Lampe, Nicole B. Ellison & Charles Steinfield, A Face(Book) in the Crowd: Social Searching vs. Social Browsing, CSCW '06: Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work 167 (2006).

B. Finding Obscurity in Socio-Technical Systems

In recent years, a number of studies have explored the novel challenges of privacy and disclosure management in the nonymous - and increasingly heterogenous - social media space. The problem generally explored concerns the shifting nature of privacy and disclosure management in online spaces as audiences diversify. Consider the case of Facebook – it was once a student-only network, but now crosses broad swaths of the population. How do individuals manage privacy and disclosure as audiences shift, and with these shifts, the goals and outcomes associated with sharing in the network? DiMicco and Millen, writing in 2007, described a vivid example of inherent network diversification as students move from college to their first job at a technology firm.[32] Using surveys, the authors developed social network site profile "types." – identifying a simple and highly functional disclosure management strategy. In particular, DiMicco and Millen found that people at different level of the organizational structure operate differently in social media, with adoption and disclosure levels negatively correlating with organizational embeddedness. Individuals that were more strongly embedded in the network (i.e. more senior) were more likely to have limited profiles and limit disclosures.

DiMicco and Millen's study was conducted in 2007, and adoption of Facebook was not as broad based as it is today. Later work conducted by Skeels and Grudin[33] extended this line of inquiry, analyzing the techniques individuals use to manage disclosure across multiple audiences in a similar work environment. The authors focus on the challenges of disclosing across multiple groups – as social network sites are more broadly adopted, individuals are challenged to manage disclosure across the personal networks within the social network site. One particular source of tension is the family network, and family interactions with work networks. In establishing friendships across social hierarchies, individuals are required to maintain a coherent identity across these hierarchies – a significant challenge. Work by Lampinen and colleagues[34] extensively documented

[32] Joan M. DiMicco & David R. Millen, Identity Management: Multiple Presentations of Self in Facebook, GROUP '07: Proceedings of the 2007 International ACM Conference on Supporting Group Work 383 (2007).
[33] Meredith M. Skeels & Jonathan Grudin, When Social Networks Cross Boundaries: A Case Study of Workplace Use of Facebook and Linkedin, GROUP '09: Proceedings of the ACM 2009 International Conference on Supporting Group Work 95 (2009).
[34] Airi Lampinen, Sakari Tamminen & Antti Oulasvirta, All My People Right Here, Right Now: Management of Group Co-Presence on a Social Networking Site, GROUP '09: Proceedings of the ACM 2009 International Conference on Supporting Group Work 281

some of the strategies individuals use to manage identity across network boundaries. In particular, the authors described the use of behavioral and mental strategies. Behavioral strategies include using social network sites for a single or particular purpose, matching certain tools within the network to certain communication types, "self-censoring" certain types of content. Mental strategies include the development of in-group or protected identities, as well as developing interpersonal arrangements to manage disclosure, and trust relations around disclosure.

As we have argued, the selective management of identity is a natural and commonly-occurring phenomenon, and individuals have been managing their identities online before the rise of social media. As Kling and colleagues identified, the use of simple obfuscation techniques, such as pseudonyms[35], agreements of confidentiality, relational (in-group) knowledge, and techniques of true anonymity (encryption, etc.) have been long accessible to users of Internet technology.[36] Chen and Rea extended this analysis, identifying three primary types of techniques used by online participants to manage identity disclosures.[37] First is the *falsification* of information shared online, which involves techniques such as using multiple email accounts, deleting cookies, and lying to websites. Second is *passive reaction*, which involves the use of technology to separate the identity from those making queries of the identity. Third is *identity modification*, which involves the creation of gender-neutral avatar names, and the use of throw-away online identifiers. We identify these techniques to demonstrate that active identity management has been an integral part of our experience with online disclosure, and to highlight some of the important differences introduced by the current state of Internet technology, and particularly the nonymous social Web. When an individual faces censure from her or his peer group from lying publicly, when the use of a throwaway identifier means losing one's friends list, it becomes obvious that certain extant techniques of identity protection are not available to participants in nonymous environments.

(2009).; Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio & Sakari.Tamminen, We're in It Together: Interpersonal Management of Disclosure in Social Network Services, CHI '11: Proceedings of the 29th International Conference on Human Factors in Computing Systems (2011).

[35] *See, e.g.*, Houn-Gee Chen, Charlie C Chen, Louis Lo & Samuel C. Yang, *Online Privacy Control Via Anonymity and Pseudonym: Cross-cultural Implications*, 27(3) BEHAVIOUR & INFO. TECH. 229 (2008).

[36] *See, e.g..*, Rob Kling, Ya-Ching Lee, Al Teich & Mark S. Frankel, *Assessing Anonymous Communication on the Internet: Policy deliberations*, 15(2) THE INFO. SOC'Y. 79 (1999).

[37] Kuanchin Chen & Alan I. Rea, *Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques*, 44(4) JOUR. OF COMPUTER INFO. SYS. 85 (2004).

Although a lack of access to previously existing identity protection techniques could be interpreted as a tacit dismissal of the value of these techniques, we argue that it is a catalyst for creativity. That is, individuals do not abandon their normative desire for privacy, rather, they seek privacy in contextually appropriate ways. Consider boyd's discussion of "mirror networks," one of the earliest documented "innovations" in privacy and disclosure control to emerge from social media. According to boyd, teenage users of social media sites increasingly faced the specter of surveillance from parents and other individuals of authority.[38] Rather than withdrawing from social network sites, the teenagers created densely interconnected mirror profiles – a highly sanitized copy of the profile that was densely connected within the personal friend network. In essence, these profiles created an alternate reality, where parents could snoop, and teenagers enjoyed privacy in completely separate, hidden zones of obscurity.[39]

Empirical research by Stutzman and Hartzog has explored the privacy practices of social media users, focusing particularly on those that used "multiple profiles" as an identity management strategy.[40] In a similar vein to the work of Lampinen and colleagues, this research explored the challenges of, and reaction to, increasingly heterogenous disclosure networks within social media. The use of multiple profiles, or the maintenance of one or more profiles within social network sites, represents an active "segmentation" of the social network site into multiple zones of obscurity. Most commonly, social networks were segmented along important network boundaries such as family, work, and public persona. Depending on the importance of the linkage between the personas, individuals used various techniques to "cloak" personas – such as employing privacy settings, using obscure name variants, and highly regulating the offline disclosure of the existence of the profile.

The use of multiple profiles represents an innovative approach to the challenges of disclosure within the platform, but it also represents a

[38] danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life, in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 133 (David Buckingham ed., 2008), http://www.mitpressjournals.org/doi/pdf/10.1162/dmal.9780262524834.119.

[39] In the mirror profile, the individuals are protected by multiple layers of privacy. Individuals use pseudonyms and draw heavily on protected in-group communication to cloak both the actors, and nature of the communication. This renders the networks practically "hidden" from existing techniques that could be employed to discover them, particularly text search.

[40] Frederic Stutzman & Woodrow Hartzog, *Boundary Regulation in Social Media*, Paper presented at AOIR 10: Association of Internet Researchers Annual Meeting. Milwaukee, WI. (2009), http://ssrn.com/abstract=1566904 (last accessed April 23, 2011).

fundamental failing of the platform to respect disclosure and privacy intent. Work by Lipford and colleagues attempted to rectify this through the design of technologies that adaptively match privacy intent to disclosure goals in social network sites.[41] In particular, Lipford and colleagues drew on Nissenbaum's notion of contextual integrity as a metaphor for system design. By placing the locus of control over a disclosure with the user, individuals may be better able to share in accordance with their goals and desires, and not have to react reflexively to systems and algorithms.

C. New Techniques for Existing Goals

Although the study of nonymous communication environments is nascent, as Zhao and colleagues point out, there is good evidence that supports the emergence of privacy enhancing practice in these sites. In particular, individuals exert control over the information disclosed by limiting the audience of the disclosure, by bounding the meaning of the disclosure, and by reflexively adapting the disclosure to the site. In these sites, where the use of anonymity would violate norms and limit benefits attained from site use, individuals strategically develop techniques that effectively produce obscurity in disclosure. This is not to say that established techniques of privacy management are invalid in these domains – but rather that new techniques that are contextually appropriate emerge so individuals can maintain normative expectation of privacy and obscurity.

Considering the existence of a powerful popular discourse that argues that individuals online have essentially different privacy and notoriety goals,[42] it is essential that we provide evidence that the finding of obscurity online is normative and expected. Therefore, the previous two sections have attempted to demonstrate that online obscurity is a crucial aspect of privacy for Internet users. Through obfuscation techniques and other normative practices, it is clear that obscurity is desired and expected online. The next section discusses how, even though obscurity is a central aspect of online privacy, the concept is languishing in privacy law.

[41] *See, e.g.*, Andrew Besmer & Heather Richter Lipford, Moving Beyond Untagging: Photo Privacy in a Tagged World, Proceedings of the 28th international conference on Human Factors in Computing Systems 1563 (2010); Heather R. Lipford, Gordon Hull, Celine Latulipe, Andrew Besmer & Jason Watson, Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites, Computational Science and Engineering, CSE '09. International Conference on, 4, 985 (2009); Katherine Strater & Heather R Lipford, Strategies and Struggles with Privacy in an Online Social Networking Community, Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1, 111 (2008).

[42] *See, e.g.*, Emily Nussbaum, *Say Everything*, NEW YORK MAGAZINE, (Feb. 12, 2007), 24-29, 102-103, http://nymag.com/news/features/27341/.

III. THE SPECTER OF OBSCURITY IN ONLINE PRIVACY LAW

The well-documented problem with the current state of privacy law is that it simply does not reflect societal or individual notions of privacy.[43] The purpose of this section is to demonstrate how the law has failed to embrace or develop the concept of online obscurity. Even when obscurity seems implicit in a number of disputes, courts seem to wrap it into larger or different concepts of privacy law, such as confidentiality and "public information." Although the disconnect between law and individual notions of privacy has been approached from a number of angles by courts and scholars, a large number of conflicts seem to stem from one problem: individuals have complex notions of privacy in personal information but the law treats that information only two ways: public or private. This maligned on/off approach to privacy has been called the "public/private dichotomy"[44] or "secrecy paradigm."[45]

Although this dichotomy has distorted the societal expectations of privacy before the Internet, it has proven to be even more unworkable online. This section seeks to highlight the failure of courts and lawmakers to embrace online obscurity. The need for a workable concept of online obscurity is no more important than when courts attempt to determine what "public" online information is. This section will first review the public/private dichotomy in privacy law and critics' critique as to why it is flawed. As an example of how the law has failed to embrace the concept of obscurity, this section will explore case law that seeks to determine whether online information is "public." Finally, this section will examine a few of the statutes and regulations that implicitly value obscurity as a means to protect privacy, but fail to adequately conceptualize it.

A. The Public/Private Dichotomy

In his book *The Digital Person*, Daniel Solove described the "secrecy paradigm" as an understanding of privacy based on concealment

[43] *See, e.g.,* DANIEL SOLOVE, UNDERSTANDING PRIVACY (2008); HELEN NISSENBAUM, PRIVACY IN CONTEXT (2009); Helen Nissenbaum, *Protecting Privacy in the Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004); Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002); Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

[44] HELEN NISSENBAUM, PRIVACY IN CONTEXT (2009); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

[45] DANIEL SOLOVE, THE DIGITAL PERSON 42 (2004).

preventing others from invading one's hidden world.[46] Under this conception, disclosed information is no longer concealed and, thus, no longer private. Sharon Sandeen noted that this vision of privacy "makes it difficult for individuals to protect personal information once it has been shared with others."[47] Solove argued that the secrecy paradigm "fails to recognize that individuals want to keep things private from some people but not others."[48] Obscurity can play a key role in such situations online.

Disclosing information to some, but not all, is difficult in modern society. Solove asserted that not all private activities are pure secrets "in the sense that they occur in isolation and in hidden corners. When we talk in a restaurant, we do not expect to be listened to. A person may buy condoms or hemorrhoid medication in a store open to the public, but certainly expects these purchases to be private activities."[49]

Solove has recognized the utility of obscurity. Regarding doctrinal notions of "public," Solove asserted that even though many argue that public records cannot be considered private, "there is a considerable loss of privacy by plucking inaccessible facts buried in some obscure [public] document and broadcasting them to the world on the evening news. Privacy can be infringed even if no secrets are revealed and even if nobody is watching us."[50] In other words, context is important when considering whether information is considered "public" or "private." Solove and other scholars have pondered whether secrecy is even possible in a networked world. In a separate article, Solove posited that life in the Information Age "often involves exchanging information with third parties, such as phone companies, Internet service providers, cable companies, merchants, and so on. Thus, clinging to the notion of privacy as total secrecy would mean the practical extinction of privacy in today's world."[51]

Helen Nissenbaum asserted that the labeling of information as exclusively public or private (what she refers to as the public/private dichotomy) fails to consider context, which rationalizes an individual's

[46] *Id.*

[47] Sharon Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 694 (2006). Online obscurity has also appeared in the trade secret literature. *See* Elizabeth A. Rowe, *Saving Trade Secret Disclosures On the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1, 17-21 (2007). Rowe asked the question of trade secret doctrine "Does public mean public accessibility or public publication? Does the obscurity of the Web site matter, or are all Internet postings equal?...The precise measure of obscurity or transience required to protect the trade secret, however, is unsettled." *Id.*

[48] DANIEL SOLOVE, THE DIGITAL PERSON 44 (2004).

[49] *Id.*; *see also infra* Sections I and II.

[50] *Id.*

[51] Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1152 (2002).

desire to have "privacy in public."[52] According to Nissenbaum, the relegation of information into public and private "spheres" is rife with challenges, as "[i]nterpretations of what counts as a private space may vary across times, societies, and cultures."[53] Nissenbaum observed that the common rebuttals to claims of privacy in public are:

> [W]hen people move about and do things in public arenas, they have implicitly yielded any expectation of privacy. Much as they might prefer that others neither see, nor take note, expecting others not to see, notice, or make use of information so gained would be unreasonably restrictive of others' freedoms. One cannot reasonably insist that people avert their eyes, not look out their windows, or not notice what others have placed in their supermarket trolleys. And if we cannot stop them from looking, we cannot stop them remembering and telling others. In 2001, Tampa police, defending their use of video cameras to scan faces one-by-one as they entered the Super Bowl stadium, stated, "the courts have ruled that there is no expectation of privacy in a public setting."[54]

In essence, information that falls within the private half of the public/private dichotomy warrants privacy consideration; "for all the rest, anything goes."[55]

Nissenbaum also rejected the public/private distinction in law. Instead, she created a framework of privacy called "contextual integrity," based on the central tenet that "there are no arenas of life not governed by norms of information flow, no information or spheres of life for which 'anything goes.'"[56] Thus, the idea that information can objectively be "public" or categorically undeserving of privacy protection is countered by the fact that "[a]lmost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation."[57] According to Nissenbaum, the integrity of these contexts is maintained when norms of appropriateness and flow or distribution are maintained, and that this

[52] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT (2009); Helen Nissenbaum, *Protecting Privacy in the Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

[53] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 132 (2004).

[54] *Id.* at 135-36.

[55] *Id.*

[56] *Id.* at 136.

[57] *Id.* at 137.

maintenance of contextual norms is the hallmark of privacy.[58] As will be discussed in Section IV, our proposed definition and framework for online obscurity is based on Nissenbaum's theory of contextual integrity.

Other scholars commenting on the secrecy paradigm have noted the practical and constitutional difficulty in defining the term "public" in order to determine if information is worthy of privacy protections.[59] Dianne Zimmerman noted that "to distinguish private facts from 'public' information about an individual, courts often look either to the location of the action or to the nature of the subject matter. Courts using the 'location' analysis commonly state that information individuals reveal about themselves in public places is by definition not private."[60] Courts using the subject matter analysis "rule that the subject matter is private even though the locus is not."[61] Zimmerman found that both approaches are practically unfeasible and threaten freedom of speech.

Not all scholars have found the public/private dichotomy problematic. In her article *The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public*, Heidi Reamer Anderson defines obscurity simply as "the absence of exposure."[62] Anderson defended the public/private dichotomy and argued that it has some benefits. According to Anderson, this definition helps with the "obscurity problem," which occurs when a private actor lawfully collects and further exposes information that someone else initially shared in public.[63] However, this definition of obscurity is unhelpful for the purposes of this article, because it relies on the same conception of "public" as the public/private dichotomy. Thus, it does not reflect the research that demonstrates the significant role obscurity plays in the disclosure of information online. As we tried to demonstrate in Part II of this article, obscurity is not simply an incidental

[58] *Id.*

[59] Diane Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291 (1983); Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97 (2000); 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).

[60] Diane Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 347 (1983).

[61] *Id.* at 349.

[62] Heidi Reamer Anderson, *The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public*, JOUR. OF LAW & POL'Y FOR THE INFORMATION SOCIETY (forthcoming), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1759374 (last accessed September 5, 2011).

[63] *Id.* Anderson ultimately concluded that "a potential loss in obscurity is a small price to pay for [benefits the gained from transparency] and that the 'no privacy in public' rule remains valid.'"

benefit conferred when disclosing information online; it is a crucial aspect influencing disclosure and regularly relied upon by Internet users.

The public/private dichotomy in the law is flawed because it relies on largely arbitrary distinctions that fail to reflect Internet users' notions of privacy. Courts faced with Internet privacy disputes too often simply shuttle online information into one category or another with little discussion as to why. Perhaps even more problematic, courts and lawmakers rely too much on one specific technology, like passwords, to define what information is public. As the following sections demonstrate, privacy disputes are littered with examples of online obscurity, yet courts fail to recognize the concept. A concrete and usable definition of obscurity would better help courts and lawmakers resolve privacy disputes by better reflecting the reality of the online disclosure of information.

B. Obscurity: The Elephant in the Courtroom

Courts have not explicitly embraced the concept of online obscurity, but its existence is hard to ignore in a number of disputes. This section will detail how judicial support for the analog version of online obscurity – practical obscurity – has laid the foundation for the recognition of online obscurity. This section will also explore how obscurity has been glossed over in online disputes where courts attempt to define information as public or private. This section will look at different obfuscation techniques or contexts like barriers to access such as passwords, privacy settings, and encryption; shared or networked access to online information; and search visibility.

Applying the public/private dichotomy, courts have seemed to reach one common conclusion – the unfettered ability of any hypothetical individual to find and access information on a website renders that information "public," or ineligible for privacy protection. Finally, this section details the problematic tendency of courts rely passwords to define what information is public – another reason a workable definition of online obscurity is needed.

1. Practical Obscurity

Online obscurity has an older sibling - "practical obscurity." This concept, which typically focuses on offline impediments to data retrieval, was articulated by the Supreme Court in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*.[64] In evaluating the privacy of a "rap sheet" containing aggregated public records, the Supreme Court

[64] 489 U.S. 749, 770 (1989).

found a privacy interest in information that was technically available to the public, but could only be found by spending a burdensome and unrealistic amount of time and effort in obtaining it.[65] The information was considered practically obscure because of the extremely high cost and low likelihood of the information being compiled by the public. Thus, practical obscurity became a recognized concept in privacy doctrine. Yet, this concept remains underdeveloped. The doctrine has largely been confined to disputes involving access to public records,[66] computer security,[67] and governmental

[65] *Id.* at 764. The court found:

> The very fact that federal funds have been spent to prepare, index, and maintain these criminal-history files demonstrates that the individual items of information in the summaries would not otherwise be "freely available" either to the officials who have access to the underlying files or to the general public. Indeed, if the summaries were "freely available," there would be no reason to invoke the FOIA to obtain access to the information they contain. Granted, in many contexts the fact that information is not freely available is no reason to exempt that information from a statute generally requiring its dissemination. But the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information.

Id.

[66] Peter A. Winn, *Judicial Information Management in an Electronic Age: Old Standards, New Challenges*, 3 FED. CTS. L. REV. 135 (2009); Caren Myers Morrison, *Privacy, Accountability and the Cooperating Defendant: Towards a New Role for Internet Access to Court Records*, 62 VAND. L. REV. 921 (2009); Lewis A. Kaplan, *Litigation, Privacy and the Electronic Age*, 4 YALE SYMP. ON L. & TECH 1 (2001) ("This practical obscurity of information generated in all but the most exceptional cases has been eroded by technological advances."); Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 301 (2003) ("Digital technology is turning the asset of open government into a privacy nightmare. In the analog age, public records were all available, but languished in 'practical obscurity' in courthouse basements or isolated file cabinets."); Kristen M. Blankley, Note, *Are Public Records Too Public? Why Personally Identifying Information Should be removed from Both Online and Print Versions of Court Documents*, 65 OHIO ST. L.J. 413 (2004). Arminda Bradford Bepko, Note, *Public Availability or Practical Obscurity: The Debate Over Public Access to Court Records on the Internet*, 49 N.Y.L. SCH. L. REV. 967 (2004).

[67] Computer security through obscurity involves a slightly different set of concerns than user privacy. Obscurity is not favored as a computer security technique. *See,e.g.,* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA. L. REV. 1701, 1724 (2010) ("Not only do reidentification scientists spurn security through obscurity, but they often assume that the adversary possesses the exact piece of data--if it exists--needed to unlock anonymized identities, in order to design responses that protect identity even in this worst case."); *cf*, Peter Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1350-51 (2006) ("'Obscurity is camouflage, security is armor.' Either can be useful, depending on the circumstances. They can also be useful when working together, much as tanks are often camouflaged.").

searches.[68] Beyond a general sense that shared or available information does not always constitute public information, courts have had a difficult time expanding upon the concept.[69]

The doctrinal support for practical obscurity forms the foundation for utilizing the concept of obscurity in online disputes [70] In *Burnett v.*

[68] A few have advocated online obscurity in context of governmental searches. *See* Dave Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009). Couillard also argued for a recognition of online obscurity, stating:

> Courts should…acknowledge the legitimacy of virtual concealment efforts-- encryption, password protection, and the practical obscurity of unlisted links--as means of opacity in the cloud context. Under this rule, courts would make a case-by-case determination as to whether a user's reliance upon a password, encryption, or obscurity was a reasonable effort to conceal in a given situation. It is not a burden for law enforcement to determine whether a password is necessary to access a website, at which point it would need a warrant prior to accessing the account. Conversely, in the unlisted-link context, if an unlisted address appears on a public website as a hyperlink, law enforcement should be given discretion to treat such a virtual container as in plain view.

Id. at 2236; *see also* Matthew Hodge, Comment, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and Myspace.com*, 31 S. ILL. U. L.J. 95, 108 (2006) ("[A] user could only try to argue that a MySpace profile is not public knowledge, and that it is so obscure as to force the police to go searching for the profile. This obscurity…could be argued to deem some expectation of a private area."); Carla Scherr, *You Better Watch Out, You Better Not Frown, New Video Surveillance Techniques are Already in Town (and Other Public Spaces)*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 499, 506 (2008) ("The concept of "practical obscurity" applies to public information that is usually outside the public consciousness because it is contained in a large number of individual pieces that are practically impossible to accumulate and organize, or because it is impossible to find, for example a paper document stored in the dusty basement of the local courthouse or in an infinitely large government warehouse.").

[69] A number of scholars have argued that the traditional notion of practical obscurity, which relied on offline impediments to discovery, no longer exists in a digital world. *See, e.g.*, Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 501 (2010) ("While before there was a fair amount of practical obscurity of information gathered in a public place, today the potential for immediate global dissemination of that information is unprecedented. Once information is available online, it is impossible to put the genie back in the bottle."); Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1100-01 (2002) (stating "while the scattering of information throughout numerous computer databases had preserved some practical obscurity, the Internet has all but eliminated those remnants of isolation."); Omar Tene, *What Google Knows: Privacy and Internet Searches,* 2008 UTAH L. REV. 1433, 1440 (2008) ("Before…search engines, we enjoyed a degree of "practical obscurity," [Information] was protected de facto from all but skilled investigators or highly motivated researchers, due to the practical difficulty and costs involved in uncovering and compiling the data. Today such information has become available instantly and free of charge through search engines….").

County of Bergen,[71] the Supreme Court of New Jersey ordered the redaction of social security numbers from court records because their inclusion with other personal information elevated privacy concerns. Even though these social security numbers were freely available to the public in the clerk's office, the court noted that the "bulk disclosure of realty records to a company planning to include them in a searchable, electronic database would eliminate the practical obscurity that now envelops those records at the Bergen County Clerk's Office."[72]

The court cited *Reporter's Committee*, which held that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[73] The court went on to say that "composite documents – in this case records that would be made available in a searchable computer database - implicates privacy concerns much more broadly than documents with one item alone."[74]

This same principle compelled the Supreme Court of Michigan in *Michigan Federation of Teachers v. University of Michigan*[75] to conclude that university employees' home addresses and telephone numbers were protected by the Michigan FOIA's privacy exemption. The court stated:

> It is true that home addresses often are publicly available through sources such as telephone directories and voter registration lists, but "[i]n an organized society, there are few facts that are not at one time or another divulged to another." The privacy interested protected by [the federal exemption] "encompass[es] the individual's control of information concerning his or her person." An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form.[76]

[70] *See, e.g.*, Burnett v. County of Bergen, 968 A.2d 1151 (N.J. 2009); Lambert v. Hartmann, 898 N.E.2d 67 (Ohio Ct. App. 2008); Finnerty v. State Bank and Trust Co., 687 S.E.2d 842 (Ga. Ct. App. 2009); *In re* French, 401 B.R. 295 (E.D. Tenn. 2009).

[71] 969 A.2d 1151 (N.J. 2009).

[72] *Id.* at 1164.

[73] *Id.* (citing United States Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 764 (1989)).

[74] *Id.*

[75] 753 N.W.2d 28 (2008).

[76] *Id.* at 679 (citing United States Dep't of Defense v. Fedl. Labor Relations Auth., 510 U.S. 487, 500 (1994)).

The court reasoned that "[a]n individual's home address and telephone number might be listed in the telephone book or available on an Internet website, but he might nevertheless understandably refuse to disclose this information, when asked, to a stranger, a co-worker, or even an acquaintance."[77] This analysis recognizes the value of obscure information. Employees addresses and phone numbers were freely accessible by those seeking to find them, but were obscure in certain contexts and, thus, not "public."

While many cases support the concept of "practical obscurity," which usually involves offline limitations to accessing information, courts have been less receptive to a purely online concept of obscurity. Instead, they typically rely on the secrecy paradigm. In the case of *Yath v. Fairview Clinics*, the Court of Appeals of Minnesota wrote that:

> It is true that mass communication is no longer limited to a tiny handful of commercial purveyors and that we live with much greater access to information than the era in which the tort of invasion of privacy developed. A town crier could reach dozens, a handbill hundreds, a newspaper or radio station tens of thousands, a television station millions, and now a publicly accessible webpage can present the story of someone's private life, in this case complete with a photograph and other identifying features, to more than one billion Internet surfers worldwide.[78]

In *J.S. v. Bethlehem School District*, the Commonwealth Court of Pennsylvania stated that "the creator of a web-site controls the site until such time as it is posted in the Internet. Once it is posted, the creator loses control of the web-site's destiny and it may be accessed by anyone on the Internet. Without protecting the web-site, the creator takes the risk of other individuals accessing it once it is posted."[79]

This kind of analysis reflecting a perceived omnipresent disclosure is typical of the case law regarding "public" information. Yet it presents a false dichotomy between complete worldwide dissemination and near total secrecy. Website users have many different tools to regulate access and dissemination of information. They can disclose only to certain users by activating privacy settings, protect their website with a password, and de-list their website from search engines with robot.txt files.[80] As will be

[77] *Id.*

[78] Yath v. Fairview Clinics, 767 N.W.2d 34, 44 (Minn. Ct. App. 2009).

[79] J.S. v. Bethlehem Area School District, 757 A.2d 412, 425 (Pa. Commow. Ct. 2000).

[80] *See infra* note 145.

discussed in Part IV, the concept of online obscurity could be expanded and clarified, which would make it more useful. The next two sections will explore cases where courts have either ignored obscurity or limited their analysis of the concept to technological restrictions like passwords.

2. Unlimited Access

Courts typically presume that online information that could be found and accessed by anyone is public information.[81] A good example of this tendency is *United States v. Gines-Perez.*[82] In *Gines-Perez,* the U.S. District Court for Puerto Rico was asked to determine if use of a photograph downloaded by police from a website violated an individual's right to privacy. The defendant claimed that the downloaded picture was obtained from an alleged "private" website. Specifically, the defendant claimed that the general public could not access the site, that it was not being used for commercial purposes, and that it was under construction.[83]

The court found that the defendant had no subjective or reasonable expectation of privacy in the photographs posted online.[84] The court unequivocally ruled that "placing information on the information superhighway necessarily makes said matter accessible to the public, no matter how many protectionist measures may be taken, or even when a web

[81] *See, e.g.,* United States v. Gines-Perez, 214 F. Supp. 2d 205 (D.P.R. 2002); Moreno v. Hanford Sentinel, 172 Cal. App. 4th 1125, 1130 (Ct. App. 5th Dist. 2009); Boring v. Google, 2010 WL 318281 (3rd Cir.); Yath v. Fairview Clinics, 767 N.W.2d 34 (Minn. Ct. App. 2009); Sandler v. Calcagni, 565 F.Supp.2d 184 (D. Maine 2008); State v. Birchfield, 2007 WL 147235 (N.J. Super.A.D.); Four Navy Seals v. Associated Press, 413 F. Supp. 2d 1136 (S.D.Cal. 2005); Guest v. Leis, 255 F.3d 325 (6th Cir. 2001) ("Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."); United States v. D'Andrea, 497 F. Supp. 2d 117 (D. Mass. 2007).

[82] 214 F. Supp. 2d 205 (D.P.R. 2002).

[83] 224.

[84] The "reasonable expectation of privacy" test is a complex and often maligned doctrine requiring analysis beyond the scope of this paper. It is sufficient for the purposes of this paper to acknowledge that courts generally hold that individuals do not have a reasonable expectation of privacy in "public' information for Fourth Amendment purposes. Donald Pongrace, *Stercotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 AM. U. L. REV. 1191 (1985). For more information, *see, e.g.,* Daniel Solove, *Fourth Amendment Pragmatism,* 51 B.C. L. REV. 1511 (2010); Gerald G. Ashdown, *The Fourth Amendment and the 'Legitimate Expectation of Privacy,'* 34 VAND. L. REV. 1289 (1981); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy,* 55 STAN. L. REV. 119 (2002); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077 (1987); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007).

page is 'under construction.'"[85] The court noted that the intention of the communicator in posting information online is irrelevant. Instead, "it is the medium in which he or she places the information and the nature of the materials placed on the Web which are important. A person who places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party."[86]

Regarding the reasonableness of a claim to privacy, the court found a "reasonable person cannot place 'private' information -- such as a 'private' photograph -- on the Internet, if he or she desires to keep such information in actual 'privacy.' A reasonable person does not protect his private pictures by placing them on an Internet site."[87] Despite earlier declaring the intent of the discloser irrelevant, the court then pronounced that society would most likely recognize "that a person who places a photograph on the Internet precisely intends to forsake and renounce all privacy rights to such imagery, particularly such as here, where Defendant did not employ protective measures or devices that would have controlled access to the Web page or photograph itself."[88] As we argued in Section II, empirical research demonstrates that users do not intend to renounce privacy rights when posting on the Internet. Yet this type of analysis persists.

Other courts have concurred with the sentiment laid out in *Gines-Perez.* In *Sandler v. Calcagni,*[89] the U.S. District Court for the District of Maine held that information contained on a "publicly accessible myspace.com webpage" was not a private fact. In *State v. Birchfield,*[90] the Superior Court of New Jersey held that "defendant has no reasonable expectation of privacy in [a] chat room, which was conducted as an open discussion forum which any adult member of the public could join."[91]

In *Four Navy Seals v. Associated Press,*[92] the U.S. District Court for the Southern District of California was asked to consider whether military personnel could consider website photos found by a journalist via a search engine and accessed and downloaded "without the necessity of keying in any password, entering a code or incurring a monetary charge" to be private.[93] The court found that the journalist's "act of downloading photos from a publicly-accessible website…was not an egregious breach of social

[85] *Gines-Perez,* 214 F. Supp. 2d at 225.
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] 565 F. Supp. 2d 184 (D. Maine 2008).
[90] 2007 WL 147235 (N.J. Super.A.D.).
[91] *Id.* at *3.
[92] 413 F. Supp. 2d 1136 (S.D. Cal. 2005).
[93] *Id.* at 1142.

norms underlying the state privacy right."[94] Rather, it found that "one cannot reasonably expect the internet posting of photos to be private."[95] As will be discussed, search visibility is a critical component of online privacy, but the court should not simply consider availability as the sole factor in their analysis.

Barriers to access are also effective and forceful tools for the creation and maintenance of online obscurity. For courts, however, these barriers, particularly passwords, often seem to be the only obscurity factor considered. The following cases demonstrate how courts can recognize that while completely unprotected websites were ineligible for privacy protection, restricted websites might be considered private under various thresholds. Yet, without a definition of online obscurity, the cases reveal that courts are likely to end their analysis after considering barriers to access such as passwords and encryption. This refusal to consider other factors of obscurity has seemingly resulted in the unspoken general rule that password-restricted disclosures are private, and all other disclosures online are public.

In *Gines-Perez*, the court held that "it strikes the court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably public medium, such as the Internet, **without taking any measures to protect the information**."[96] In *Pietrylo v. Hillstone Restaurant Group*,[97] the U.S. District Court for the District of New Jersey was asked to determine the privacy interest in information contained on a "closed" webpage on the social network site MySpace.com. An employee at a local restaurant created a group to vent about his employer "without any outside eyes spying in on [them]"[98] The website creator stated that "[t]his group is entirely private, and can only be joined by invitation." The court noted that the icon for the group, which was the restaurant's trademarked logo, "would appear only on the MySpace profiles of those who were invited into the group and accepted the invitation."[99]

Because each member accessed her or his own profile by entering in a username and password, the creator effectively restricted the website to authorized users in possession of an invitation to the group and a password-protected MySpace profile. One of the invited users disclosed her password to her managers at the restaurant, which resulted in a lawsuit by the group creator alleging that the managers violated the group's privacy. The court

[94] *Id.* at 1143.
[95] *Id.* at 1147.
[96] United States v. Gines-Perez, 214 F. Supp. 2d 205 (D.P.R. 2002) (emphasis in original).
[97] 2008 WL 6085437 (D.N.J.).
[98] *Id.* at *1.
[99] *Id.*

found that "[p]laintiffs created an invitation-only Internet discussion space. In this space, they had an expectation that only invited users would be able to read the discussion."[100] Here, we can see the seeds of what could become a concrete concept of obscurity.

In giving such weight to password protections, courts have in some ways already laid the groundwork for online obscurity. In *United States v. D'Andrea,*[101] the U.S. District Court for the District of Massachusetts "seemed to presume that the password protection [of a website] was sufficient to afford a reasonable expectation of privacy."[102] The court cited Professor Warren LaFave, a "preeminent authority of the Fourth Amendment," who "argues that a person who avails herself of a website's password protection should be able to claim a reasonable expectation of privacy in the site's contents."[103] LaFave asserted that "[r]reliance on protections such [as] individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is penetrable."[104]

In *Kelleher v. City of Reading*,[105] the U.S. District Court for the Eastern District of Pennsylvania concluded that an employee might have a reasonable expectation of privacy in e-mail communications, depending upon the circumstances of the communication and the configuration of the e-mail system – seemingly an allusion to password protection. The U.S. Court of Appeals for the Armed Forces supported privacy in e-mails protected by passwords in *United States v. Long*,[106] stating "we find that password protection…support[s] the lower court's conclusion that Appellee met her burden of demonstrating a subjective expectation of privacy."[107]

Several courts have considered whether a computer shared files or access over a network relevant in determining if the information on a computer was "public."[108] In *United States v. Stults,*[109] the U.S. Court of

[100] *Id.* at *6.
[101] 497 F. Supp. 2d 117 (D.Mass. 2007).
[102] David Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2227 (2009).
[103] *D'Andrea*, 497 F.Supp.2d at 121.
[104] *Id.* (citing LaFave, 1 *Search and Seizure* § 2.6 at 721 (4th ed. 2006)).
[105] 2001 WL 1132401 at *5 (E.D. Pa.).
[106] 64 M.J. 57 (C.A.A.F. 2006).
[107] *Id.* at 64.
[108] *See, e.g.* Interscope Records v. Duty, 2006 WL 988086 (D. Ariz.) (stating that "it is undisputed that the shared file is publicly available, therefore the [counterclaimant] cannot show that the Recording Companies intruded upon her private affairs [by accessing the file sharing folder on her computer]"); United States v. Durdley, 2010 WL 916107 (N.D. Fla.) (finding that the accidental sharing of files over a computer network and thumb drive left in

Appeals for the Eighth Circuit held that an individual had no reasonable expectation of privacy in files retrieved from that individual's personal computer where software was used to "make his files accessible to others for file sharing."[110] The court drew an offline analogy, stating, "one who gives his house keys to all of his friends who request them should not be surprised should one of them open the door without knocking."[111] The court focused on the fact that the individual had opened his computer to "anyone else with the same freely available program" and thus "opened up his download folder to the world."[112]

The U.S. District Court for the District of Oregon reached a similar conclusion in *United States v. Ahrndt*,[113] finding that an unsecured wireless network and iTunes folder configured to share access with any surrounding computers utilizing the same software defeated a claim for a reasonable expectation of privacy.[114] Courts' general emphasis on closed or restricted systems shows their willingness to protect information that is shared with some but not all. A useful definition of obscurity would be consistent with this logic while expanding the scope of protection for Internet users.

3. Search Visibility

For some courts, whether a website could be located via a search engine was relevant in determining whether information was public. For example, in *Four Navy Seals*, the court explicitly noted that the degree of intrusion by a reporter was minimal because she "merely conducted a search on the internet, and used no deception in locating and downloading the images."[115] In *J.S. v. Bethlehem Area School District*,[116] the Commonwealth Court of Pennsylvania ruled that a student maintained no reasonable expectation of privacy in a website he created because the student's website was not protected, "meaning that only certain viewers could access the site by use of a known password. As such, any user who happened upon the correct search terms could have stumbled upon Student's web-site. For example, a search of the terms 'Bethlehem Area

a common use computer destroyed a reasonable expectation of privacy)(citing United States v. King, 509 F.3d 1338 (11th Cir. 2007)).

[109] 575 F.3d 834 (2009).

[110] *Id.* at 843.

[111] *Id.*

[112] *Id.* (citations omitted).

[113] 2010 WL 373994 (D.Or.).

[114] *Id.* at *3-9.

[115] *Four Navy Seals*, 413 F. Supp. 2d at 1145.

[116] 757 A.2d 412, 425 (Pa. Commow. Ct. 2000).

School District' may have found Student's site in its results."[117] This focus on search visibility adds a layer to the public/private analysis that cuts against the secrecy paradigm and instead focuses on contextual factors and the reality of how individuals find information and communicate online. This factor should be further utilized by more courts. While some courts considered search visibility as something that can make information public, search invisibility has yet to be developed as a concept that can render information private.

C. The Obscurity Interest in Statutes and Regulations

Lawmakers have also implicitly recognized the value of obscurity, but their failure to embrace it as a concept has resulted in criticism that their laws fail to protect "privacy"—meaning secrets—or that they protect information that is not private at all. If lawmakers were to clarify that they were seeking to protect the obscurity of information, these laws might be perceived and implemented differently.

Laws that implicitly value obscurity often protect information that can be discovered or understood by those in the right situation. For example, the Drivers Privacy Protection Act[118] prohibits the disclosure of information about any individual obtained by the DMV in a motor vehicle record. Of course, much of the information protected by this statute, such as home address, height, and hair color, is hardly secret, or even private. But the law implicitly protects whatever obscurity the information exists in by restricting access to it. A similar logic applies to the Video Privacy Protection Act,[119] which prohibits videotape service providers from disclosing information such as an individual's rental history. Other videotape shoppers might be able to observe an individual renting a particular movie in public, but that information would be largely unknown, and this law can be seen as supporting that obscurity. Financial and commercial privacy laws often restrict the disclosure of "personal information" or "personally identifiable information," which, while often private, often includes information that is hardly a secret.[120] A recent dispute resulted in a determination that even a zip code qualified as protected information.[121] Critics of this decision failed to see how a zip code

[117] *Id.*

[118] 18 U.S.C. §§ 2721-2725 (1994).

[119] 18 U.S.C. § 2710 (1988).

[120] *See, e.g.* California Breach Notification Statute, Cal. Civ. Code §§ 1798.29, 1798.82, 1798.84 (2002); Massachusetts Breach Notification Statute, 201 CMR § 17.00; California Data Security Breach Statute, Cal. Civ. Code §§ 1798.81.5 (2004).

[121] Bob Elelko, *Stores can't ask for ZIP codes at time of purchase*, SAN FRANCISCO CHRONICLE (Feb. 11, 2011), http://www.sfgate.com/cgi-

could be private.[122] Using the term "privacy" might be more confusing than clarifying in this case. It might make more sense to justify the decision as a protection of the obscurity of information that, if linked to other information, could be harmful to an individual. In this way, obscurity can protect against the misuse of personal information.

Many of these disputes trace back to the larger debate of "privacy in public." A full critique of this topic is beyond the scope of this paper and has been well-addressed by others.[123] However, for statutes that attempt to address privacy issues involving "public" information online, we suggest that in some instances it is not privacy generally, but specifically obscurity, that these laws should explicitly support or protect.

In sum, courts and lawmakers have not explicitly embraced online obscurity, although the concept is implicit in a number of privacy disputes. Obscurity has been derided as misguided[124] or ineffective in actually addressing privacy concerns,[125] but that label is often unfair and inaccurate

bin/article.cgi?f=/c/a/2011/02/10/BUDF1HLGJM.DTL&type=business; Pineda v. Williams Sonoma, 51 Cal.4th 524, 2011 WL 446921. (Cal.).

[122] *See, e.g.*, Kashmir Hill, *A Ridiculous California Court Ruling: Zip Codes are Private*, FORBES (Feb. 11, 2011), http://blogs.forbes.com/kashmirhill/2011/02/11/a-ridiculous-california-court-ruling-zip-codes-are-private/; *cf* Chris Hoofnagle, *Pineda and the Law of the Jungle*, TECHNOLOGY—ACADEMICS—POLICY (Mar. 8, 2011), http://www.techpolicy.com/PinedaLaw-of-Jungle_Hoofnagle.aspx.

[123] *See, e.g.,* Solove, *supra* note 43; Nissenbaum, *supra* note 43;

[124] *See, e.g.,* Martin E. Halstuk & Charles N. Davis, *The Public Interest Be Damned: Lower Court Treatment of the Reporters Committee 'Central Purpose' Reformulation,* 54 ADMIN. L. REV. 983 (2002)("[T]he Reporters Committee "central purpose" definition and theory of "practical obscurity" are judicial inventions aimed at ill-defined concerns….").

[125] *See, e.g*, Richard J. Peltz & Joi L. Leonard, 59 ARK. L. REV. 555, 636 (stating that the Reporter's Committee for Freedom of the Press "condemned the theory of "practical obscurity," the notion that a limited privacy interest can be maintained in public information that is available only by sifting through files in a local courthouse and not available by more efficient and remote, electronic searches…."). Jane Kirtley has argued that in *Reporter's Committee:*

> Justice Stevens's failure to distinguish the expectation of privacy from the expectation of nondiscovery reflects the growing tendency of courts and legislatures to regard the conversion of data from paper to electronic form as having some talismanic significance. Obviously, paper documents in a file drawer are physically distinct from entries in a computer database, and the time and effort required to retrieve them differ significantly as well. Merely translating data from one form to another, however, should not alter their inherently public nature.

The EU Data Protection Directive and the First Amendment: Why a "Press Exemption" Won't Work, 80 IOWA L. REV. 639, 642 (1995); Arminda Bradford Bepko, Note, *Public Availability or Practical Obscurity: The Debate Over Public Access to Court Records On the Internet,* 49 N.Y.L. SCH. L. REV. 967, 984 (2004) ("But is a privacy right threatened when a compilation of otherwise hard to find information--what is now available in the when it is applied to online information. As discussed in Section II, obscurity is a crucial component of online privacy. Laws that support or protect the online obscurity of information could be very beneficial in many contexts. However, the utility of online obscurity is entirely dependant upon a useful conceptualization and manageable framework.

IV. DEFINITION AND FRAMEWORK FOR ONLINE OBSCURITY

The American Heritage dictionary defines obscure as "Not readily noticed or seen; inconspicuous; Not clearly understood or expressed; ambiguous or vague."[126] This understanding of obscurity is a good place to start to define online obscurity, but it is not sufficient as a doctrinal concept. Like the term "privacy," obscurity is a sweeping concept with no real doctrinal definition.[127] The term "practical obscurity," while helpful for theoretical support, is similarly unhelpful in defining online obscurity. Practical obscurity has roots in geographic or physical boundaries impeding understanding or discovery of information.[128] Given the ease of aggregation and irrelevance of physical space online, little meaning can be extracted from this concept. As previously discussed, online obscurity is concerned not with burdens but rather obfuscation. Thus, we think the proper metaphor is the key and lock.

This metaphor is likely better suited to online disputes given the judicial reliance on the digital version of the key: the password. In essence, we are simply proposing that there is more than one key that can lock information. Indeed, many kinds of keys and locks, each with varying strengths, exist, and considered cumulatively, fall along a spectrum that will allow courts to make a more nuanced analysis of online information on a scale of obscurity.

To that end, we propose the following definition: Information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We have identified four of these factors as part of a non-exhaustive and flexible list: 1) search visibility 2) unprotected access 3) identification 4) clarity. This definition draws upon the previously detailed theoretical and empirical research and requires some explication.

courthouse--is disclosed on the Internet?....[I]t does not follow that access to information alone is necessarily harmful.").

[126] *Obscure*; AMERICAN HERITAGE DICTIONARY; http://education.yahoo.com/reference/dictionary/entry/obscure (last accessed April 12, 2011).

[127] *See, e.g.*, DANIEL SOLOVE, UNDERSTANDING PRIVACY (2008).

[128] *See, infra* notes 66-68 and accompanying text.

This proposed definition of online obscurity is based on Helen Nissenbaum's theory of privacy as contextual integrity, in that the focus of the definition is on the context in which the information exists.[129] The theory of privacy as contextual integrity is the theory that privacy violations occur when the context in which information is disclosed is not respected when one person shares another's personal information.

According to Nissenbaum, the framework of contextual integrity provides that "finely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts (e.g. education, health care, and politics)."[130] Nissenbaum stated that these norms, which she referred to as "context-relative informational norms," "define and sustain essential activities and key relationships and interests, protect people and groups against harm, and balance the distribution of power."[131] Nissenbaum stated that context-relative informational norms are simultaneously reflections of expectations of privacy in certain contexts and normative prohibitions on the further dissemination of that information. [132]

Nissenbaum defined context as "structured social settings with characteristics that have evolved over time…and are subject to a host of causes and contingences of purpose, place, culture, historical accident, and more."[133] The central tenet of contextual integrity provides that "there are no arenas in life not governed by norms of information flow…. Almost everything – things that we do, events that occur, transactions that take place – happens in a context not only of place but of politics, convention, and cultural expectation."[134] Because Nissenbaum's theory focuses on context, it is well suited to frame this approach to online obscurity, which is almost entirely context-dependant.

Our conceptualization of online obscurity also draws upon Lior Strahilevitz's "Social Networks Theory of Privacy," in which he argues that an individual has a reasonable expectation of privacy where there is a low risk that the information will spread beyond the individual's social

[129] HELEN NISSENBAUM, PRIVACY IN CONTEXT (2009) (hereinafter referred to as "Context"); Helen Nissenbaum, *Protecting Privacy in the Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) (hereinafter referred to as "Integrity").

[130] Nissenbaum, Context, *supra* note 129, at 3.

[131] *Id.*

[132] *Id.* at 129.

[133] *Id.* at 130.

[134] Nissenbaum, Integrity, *supra* note 129, at 137.

network.[135] Strahilevitz has observed the value in minimizing the likelihood of discovery[136] and the benefits of obscurity.[137]

While obscurity is certainly relevant within the context of social networks, we propose that obscurity has significant utility on the Internet outside of social networks or self-disclosed information. While Strahilevitz's theory would seek to limit disclosure to certain social networks, online obscurity seeks to preserve online context regardless of an individual's relationship with others and regardless of whether the information was self-disclosed or not. Additionally, the differences between socialization and expectations of privacy are significant enough to require a conceptualization of obscurity contoured to the medium.

By focusing on obfuscation techniques that hinder discovery and comprehension, our conceptualization of online obscurity can be a manageable analytical framework with discernible criteria for all information on the Internet. Our conceptualization also envisions obscurity as a concept that is distinct from other aspects of privacy, such as confidentiality.[138] In some instances, obscurity could actually be a goal with intrinsic benefits, rather than just a metric used to define the status of information.

To reiterate, information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We adopt the dictionary definition for discovery, which is "learning something that was not known before, or of finding someone or something that was missing or hidden."[139] Comprehension is defined as "the ability to understand the information in a given context."

We have identified four of these key factors as part of a flexible list: 1) search visibility 2) unprotected access 3) identification 4) clarity. Similar to treatment of the four fair use factors, these obscurity factors should be

[135] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920-21 (2005).

[136] Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CAL. L. REV. 2007, 2040 (2010)(stating "As I explained in A Social Networks Theory of Privacy, tort law typically analyzes expectations of privacy through a probabilistic lens.").

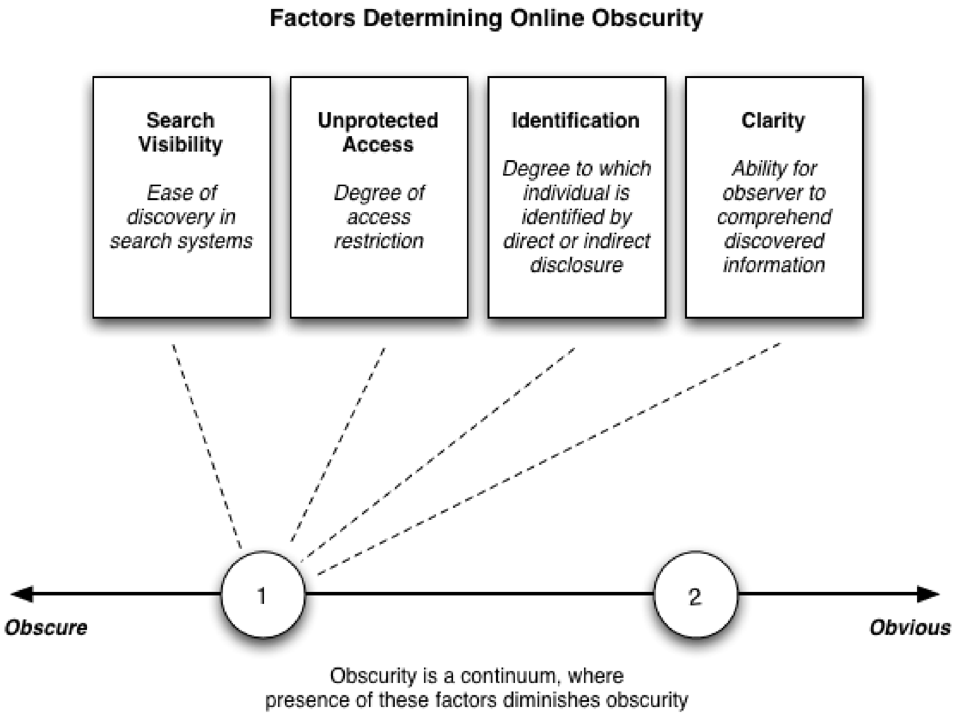
[137] Lior Jacob Strahilevitz, *Pseudononymous Litigation,* 77 U. CHI. L. REV. 1239, 1240 (2010)(proposing that "the prospect of pseudonymity in formal litigation…can be used as a device to sort grievances between informal and formal dispute resolution mechanisms.").

[138] In this way, our definition of obscurity embraces Daniel Solove's conceptualization and taxonomy of privacy as "protection from a cluster of related activities that impinge upon people in related ways." Daniel J. Solove, *A Taxonomy of Privacy,* 154 U. PA. L. REV. 477, 484 (2006); Daniel J. Solove, *Conceptualizing Privacy,* 90 CAL. L. REV. 1087(2002).

[139] *Discovery*, MACMILLAN DICTIONARY, http://www.macmillandictionary.com/dictionary/british/discovery (last accessed April 17, 2011).

considered non-exhaustive.[140] The presence of these factors diminishes obscurity, and their absence enhances it. Thus, in determining whether information is obscure online, courts should consider whether any of these factors were present in their determination. Information that is entirely un-obscure is completely obvious, and vice versa. Like in fair use disputes, courts should engage in a case-by-case analysis of the factors, examining each one individually, then as a whole to determine the degree of online obscurity.[141] Figure 1 depicts how this conceptualization would work in two different scenarios:

Figure 1


Factors Determining Online Obscurity
Search Visibility
Ease of discovery in search systems
Unprotected Access
Degree of access restriction
Identification
Degree to which individual is identified by direct or indirect disclosure
Clarity
Ability for observer to comprehend discovered information
1
2
Obscure
Obvious
Obscurity is a continuum, where presence of these factors diminishes obscurity

Scenario 1 is a blog that is visible only to invited users and is not searchable by general search engines like Google. It is close to being completely obscure because it is missing two of the most important factors for finding

[140] Copyright Act of 1976, 17 U.S.C. §107 (1976) (stating that "[i]n determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include….").
[141] *See, e.g.*, Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994)("The task [of deciding whether a work is a fair use] is not to be simplified with bright-line rules, for the statute, like the doctrine it recognizes, calls for case-by-case analysis.").

and understanding information: search visibility and unprotected access.[142] Scenario 2 is a Twitter account that uses only a first name and a blurry photo to identify the poster. While this information is more obvious than the information in Scenario 1 because it is freely searchable and accessible, it is still slightly obscure because only certain Internet users would be able to identify the poster of the content or completely comprehend any idiosyncratic posts. The following sections will develop the four factors of the framework that can erode or provide online obscurity.

A. Search Visibility

The inability to locate information through search is the one of the most significant factors in online obscurity. Search is the primary method for discovering online information, a key factor in our definition of obscurity.[143] Without search, information can only be discovered in a chain-hyperlink fashion via other websites, messages, and manual URL entry.

Yet, most online information is not visible to search engines. This information, collectively known as "the dark Web," "the deep Web" or "the invisible Web," accounts for 80-99% of the World Wide Web.[144] The dark Web doesn't just consist of websites that have been intentionally shielded from search engines using the robot.txt file.[145] It also includes websites that use privacy settings or are behind access restrictions such as passwords, which are another factor in online obscurity.[146]

[142] Note that this is similar to the MySpace group formed in *Pietrylo v. Hillstone, supra* note 97 and accompanying text.

[143] *See, e.g.*, Gary Marchionini, *Exploratory Search: From Finding to Understanding*, 49 COMMUNICATIONS OF THE ACM 41 (2006); Jamie Teevan, Susan T. Dumais & Eric Horvitz, *Potential for Personalization*, 17 ACM TRANS. COMPUTER-HUMAN INTERACT. 1 (2010); Deborah Fallows, *Search Engine Use,* PEW INTERNET & AMERICAN LIFE PROJECT (Aug. 6, 2008), http://www.pewinternet.org/Reports/2008/Search-Engine-Use/Data-Memo.aspx; Lee Raine, *Big Jump in Search Engine Use,* PEW INTERNET & AMERICAN LIFE PROJECT (Nov. 20, 2005), http://www.pewinternet.org/Reports/2005/Big-jump-in-search-engine-use/Data-Memo.aspx; Susanna Fox, *Search Engines,* PEW INTERNET & AMERICAN LIFE PROJECT (July 3, 2002), http://www.pewinternet.org/Reports/2002/Search-Engines/Data-Memo.aspx.

[144] *See supra* note 5 and accompanying text.

[145] *See, e.g.* Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 102 (2008) ("Today, nearly all Web programmers know robots.txt is the way in which sites can signal their intentions to robots, and these intentions are voluntarily respected by every major search engine across differing cultures and legal jurisdictions.").

[146] For example, the popular blogging service Blogger allows users to make their blog invisible to Google. *What do the 'listing' and 'let search engines find your blog' settings do?*, BLOGGER HELP, http://www.google.com/support/blogger/bin/answer.py?hl=en&answer=41373 (last accessed April 27, 2011). Facebook profiles that utilize privacy settings are also not found

Thus, anyone applying the concept of online obscurity should give significant weight to search visibility. A finding that information can be found via search pushes the information up the obscurity scale, closer to obvious information, making it less likely to be classified as private information. Whereas information invisible to search should be further down the scale, closer to obscurity, making it more likely to receive the benefit of privacy protections.

The breadth of the search visibility matters here. Information that is searchable at the site level is quite different than information searchable by the major Internet search engines like Google or Bing as well as the deep-Web search engines like Pipl[147] and iSearch.[148] Accordingly, if information is visible to entire Internet searches or simply more search engines, it is more obvious and less obscure.

Further explication is still required for this factor. For example, prominence in search results could conceivably affect the obscurity of information. The number or complexity of terms required to effectively find information via search could also affect the obscurity scale, although perhaps to a lesser degree. These and other mitigating factors will be addressed in future research.

B. Unprotected Access

As discussed above, in determining whether information is private, courts predominantly look to see if access to information was either unfettered or somehow restricted by technological features such as passwords and privacy settings.[149] While this approach is not sound if it is the only factor considered by courts in these disputes, it is certainly a significant part of the obscurity calculus. Not only does restricted access help prevent the discovery of information by unauthorized parties, it also serves as an indicator of the private nature of the information to those with the right credentials. Thus, barriers to access serve dual purposes of

by search engines. *How Do I Prevent Search Engines (e.g., Google) From Showing My Public Search Listing?*, FACEBOOK, https://www.facebook.com/help/?page=764#!/help/?faq=12043 (last accessed May 6, 2011).

[147] PIPL, http://www.pipl.com/ (last accessed April 16, 2011).

[148] ISEARCH, http://www.isearch.com/?refer=3338 (last accessed April 16, 2011).

[149] Restrictions to access are not limited to passwords and privacy settings. Technologies such as biometrics can also effectively restrict access to information. *See, e.g.*, Mike Elgan, *How Apple and Google will kill the password*, COMPUTERWORLD (Jan. 29, 2011), http://www.computerworld.com/s/article/9206998/How_Apple_and_Google_will_kill_the_password_.

restricting and communicating, both of which contribute to the utility of obscurity.

Conversely, the lack of restrictions to access information, particularly when they are available but unused, has the opposite effect on obscurity. A finding that information is accessible without restriction pushes the information up the obscurity scale, closer to obvious information. Information protected by passwords, privacy settings and the like should be much further down the obscurity scale, making it more likely to receive the benefit of privacy protections.

Like search, the nature of the restriction matters. Some access restrictions, like biometrics, encryption, and to a lesser degree, passwords, often trigger a rebuttable presumption of privacy by courts. However, newer access restrictions like privacy settings are diverse and evolving. In their evolution, privacy settings can also be a shifting sand, as service providers change defaults and redefine fundamental concepts of privacy within the service. Thus, these measures of privacy should be analyzed on a case-by-case basis according to how restrictive they are or can be, and in which state they were employed.

The number of people with access to information could also be a consideration here. A technological restriction that allows a small number of people to access information via passwords would make information more obscure than a privacy setting on a social network site allowing access to "friends of friends" or everyone living in a general area. As ubiquitous computing systems evolve and adoption increases, we will see moves toward dynamically generated privacy zones – privacy that is reactive to the environment and network configurations within the environment.[150] Therefore, adaptive privacy, and the audiences these adapted zones encompass, will be come increasingly important.

Solove has recognized increased accessibility, which could incorporate both the obscurity factors of search visibility and unprotected access, as a kind of privacy harm. He stated "[i]ncreased accessibility,… creates problems such as the increased possibility of disclosure. Information can readily be exploited for purposes other than those for which it was originally made publicly accessible."[151] Solove is referring to obscurity and our increasing ability to piece the puzzle together based on the range of sources we have access to online. For example, consider work that

[150] *See, e.g.*, Maomao Wu, Adaptive Privacy Management for Distributed Applications (June 2007)(Ph.D. dissertation, Lancaster University), http://eprints.lancs.ac.uk/12984/1/PhdThesis-MaomaoWu.pdf; Giovanni Iachello & Jason Hong, *End-User Privacy in Human-Computer Interaction*, 1(1) FOUNDATIONS & TRENDS IN HUMAN-COMPUTER INTERACTION 137 (2007).

[151] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV.. 477, 539 (2006).

demonstrates that social security numbers can be reasonably estimated through the piecing together of publicly available online data.[152]

C. Identification

Identification is not just one of the central aspects of online obscurity, it is one of the major components of general information privacy law.[153] Simply put, information that cannot be linked to a person poses a reduced threat to that person's privacy. Of course, the issue of anonymization and identity is significantly more complicated than that.[154] The combination of identification and obscurity is no exception. While anonymity is central to many privacy disputes, pseudonymity often gets short shrift in legal debates. Yet the use of ID variants and pseudonyms are a key component of online obscurity. Like passwords, ID variants and pseudonyms can serve two functions: 1) they can unlink content and identity to protect the discloser or subject of information and 2) if it is readily apparent that an identifying tag is an ID variant and pseudonym, it could signal to the consumer of information that the disclosure is sensitive or private.

On the social Web, where content is peer-produced in a social milieu, new challenges of identity management have emerged. On social network sites, where the articulation of the social network is a key feature, identification can occur through both direct and indirect disclosures.[155] For example, an individual that maintains a pseudononymous profile may become publicly identifiable based on whom the individual connects to, or what a friend writes on the individual's wall. Therefore, the intention of the individual in protecting her or his identity extends beyond self-disclosure, to the management of disclosures about the individual, and the selective crafting of the online persona. Identification is defined here as the existence of an irrefutable piece of information that links content online to the individual's person.

A finding that the identity of the discloser or subject of the content is clear pushes the information up the obscurity scale closer to obvious information. Whereas information associated with an ID variant or pseudonym that is not easily traceable to a real identity should be much

[152] Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106(27) PROCEEDINGS OF THE NAT. ACAD. OF SCI. 10975 (2009).

[153] *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA. L. REV. 1701 (2010).

[154] *Id.*

[155] Judith S. Donath & danah m. boyd, *Public Displays of Connection*, 22(4) BT TECH. JOUR. 71 (2004).

further down the scale closer to obscurity, making it more likely to receive the benefit of privacy protections.

D. Clarity

Often, online information is easily discoverable, but important aspects of that information are incomprehensible. Information might be intentionally vague or incomplete. Sometimes information in one domain has been separated by medium, tool or linkage from another piece in order to make it more obscure, and thus, more protected.[156] If information is too vague or incomplete, it lacks clarity, which is defined as "the ability to be easily understood."[157] Thus, a lack of clarity is a key factor of online obscurity.

As demonstrated in Part II, Internet users routinely keep information unclear in an attempt to communicate with a smaller audience while rendering information inert to a broader one. danah boyd has noted that a number of Internet users, particularly young ones, have learned how to "hide in plain sight" by "creating a message that can be read in one way by those who aren't in the know and read differently by those who are."[158] According to boyd, this process is known as "steganography," "an ancient technique where people hide messages in plain sight."[159]

Unlike identification, which focuses on the link between identity and information, clarity focuses on the link between content and some other external factor. Many kinds of information can be removed from online disclosures to create obscurity. Consider everyday communication, where shared interpersonal knowledge and linguistic styles facilitate interpersonal communication. It is because of the sharing of knowledge within groups that we can "presuppose" in conversation, as Goffman argues.[160] For the purposes of the argument, we can conceptualize clarity as the range of shared social, cultural and linguistic factors that enable presupposition. The eavesdropper at the restaurant may be able to understand some of a

[156] *See, e.g.*, Frederic Stutzman & Woodrow Hartzog, *Boundary Regulation in Social Media*, Paper presented at AOIR 10: Association of Internet Researchers Annual Meeting. Milwaukee, WI. (2009), http://ssrn.com/abstract=1566904 (last accessed April 23, 2011).

[157] *Clarity*, MACMILLAN DICTIONARY, http://www.macmillandictionary.com/dictionary/american/clarity#clarity_3 (last accessed April 17, 2011).

[158] danah boyd, *Social Steganography: Learning to Hide in Plain Sight*, ZEPHORIA (Aug. 23, 2010), http://www.zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html.

[159] *Id.* boyd gives as traditional examples "Invisible ink, tattoos under hair on messengers, and messages embedded in pictures."

[160] Erving Goffman,. *Felicity's Condition*, 89 AM. JOUR. OF SOC., 1 (1983).

conversation overheard, but there will likely be a lack of clarity that prohibits true comprehension or identification of the conversational subjects. The same is true for online communication, much of which is clouded by in-group communication that frustrates clarity.[161]

Although clarity might not be as significant a factor as search, access, and identification, it is still a valid factor in online obscurity. A finding that information was intentionally unclear to the extent that it was unlikely to be understood by unintended recipients should push it further down the obscurity scale, making it more likely to receive the benefit of privacy protections.

In sum, this conceptualization of online obscurity is broad enough to remain adaptable to new technologies and applicable in numerous contexts. However, it is also defined enough to be useful to those seeking to employ it. The next section will explore how online obscurity could be embraced in the privacy doctrine.

V. POTENTIAL APPLICATION OF ONLINE OBSCURITY

This article has attempted to demonstrate that obscurity is a central concept to online privacy that has been glossed over by courts. We hypothesized that obscurity has not been utilized in online disputes because it has not been well defined or conceptualized. Now that we have offered a useful conceptualization, it is important to consider the ways obscurity could ameliorate some of the tension between privacy law and user expectations regarding online information. Generally, online obscurity can be utilized as a frame of analysis or as part of a remedy or obligation. Specifically, the law could take advantage of online obscurity in at least three different ways: 1) as a continuum to determine whether information is eligible for privacy protections; 2) as a benefit, compromise, or procedural protection, or 3) as a duty to maintain obscurity.

It is important to emphasize that remedies utilizing the concept of online obscurity would not be a panacea for privacy harms. Online information that could cause significant and irreparable harm if plucked from obscurity should be protected by other privacy concepts such as confidentiality or by other legal doctrines. However, this does not mean obscurity is a useless concept. To the contrary, obscurity can be a meaningful legal protection precisely because it is not as protective as concepts like confidentiality or anonymity. Information that is perhaps less

[161] *See e.g.* Martin Tanis & Tom Postmes,. *Social Cues and Impression Formation in CMC,* 53 JOUR. OF COMM. 676 (2003); Joseph B. Walther, *Selective Self-Presentation in Computer-Mediated Communication: Hyperpersonal Dimensions of Technology, Language, and Cognition.* 23 COMPUTERS IN HUMAN BEHAVIOR 2538 (2007).

sensitive or sensitive in fewer contexts could be protected via obscurity if it is ineligible for more robust privacy protections.

For example, many privacy protections, such as the disclosure tort, will not apply to information known by a significant number of third parties.[162] However, the focus of online obscurity not how many people actually know of the information, but rather, the context in which the information exists. Individuals often want to protect information that might not be secrets.[163] They might not want to keep this information from being discovered or understood by everyone, they just want to keep it away from certain people. This is where obscurity becomes useful. Obscurity obligations would not aim to completely curtail the disclosure of information; rather, they would seek to minimize the likelihood of discovery, comprehension, or decontexualization. The modesty of this benefit should not overshadow its significance. Online obscurity could play a more prominent and productive role in privacy doctrine, both as an analytical tool and as part of an obligation,

A. Continuum to Determine Eligibility for Privacy Protections

Online obscurity could replace the maligned public/private dichotomy used to determine whether information is “public,” or ineligible for privacy protections. As discussed in Section III, courts generally hold that the unfettered ability of any hypothetical individual to find and access information on the Internet renders that information public. These courts generally equate accessibility with universal disclosure, invoking the mantra "if you want it kept private, it probably shouldn't be online."[164] Yet, notably,

[162] *See, e.g.*, Strahilevitz, *supra* note 135.

[163] *See, e.g.*, Daniel Solove, *“I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

[164] *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657, 2010 WL 3703242 (N.Y.Sup. September 21, 2010). The court found no reasonable expectation of privacy in social network sties, stating:

> Thus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, “[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.”

Id. (citing Dana L. Flemming and Josheph M. Herlihy, *Department: Heads Up: What Happens When the College Rumor Mill Goes OnLine? Privacy, Defamation and Online* courts often respect code-based solutions, such as passwords and encryption, which allow users to restrict access to information online. These courts acknowledge that technologically restricted access is important in determining whether information is public.

These determinations have contributed to the increasingly entrenched dichotomy where password-restricted disclosures are private, and all other disclosures online are public. This is largely an arbitrary distinction in light of how users actually perceive and expect privacy, as described in Section II. But the distinction is tempting because it is manageable for courts—it is easy to identify when users employ passwords. This is particularly true compared to the alternative; it is quite difficult to try and understand someone's "reasonable expectation of privacy" in any given context.[165] This is why any conceptualization of online obscurity must be concrete, easy to understand, manageable and as objective as possible.

Despite numerous cases on the issue, courts still lack a generally accepted framework or test to determine when online information has been made public.[166] For example, in the case *Moreno v. Hanford Sentinel,*[167] the plaintiff sought relief under the disclosure tort against a newspaper for publishing an unflattering poem about her hometown that was originally posted on the plaintiff's MySpace page. The judge denied that the poem was private because it had already been made public by the plaintiff. The judge found that the plaintiff had "publicized her opinions about [her hometown] by posting the Ode on MySpace.com, a hugely popular Internet site."

"[Plaintiff''s] affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material."[168] The judge was apparently convinced that the plaintiff's failure to utilize protective measures such as privacy settings or password protection was significant in determining whether she could reasonably expect online information to be private.

By equating "theoretically accessible" with "public," courts have failed to consider the many ways individuals obfuscate information online.

Social Networking Sites, 53 B.B.J. 16 (January/February, 2009); *see also* Moreno v. Hanford Sentinel, 172 Cal. App. 4th 1125 (2009).

[165] *See, e.g.,* Daniel J. Solove, *Fourth Amendment Pragmatism,* 51 B.C. L. REV. 1511, 1511-12 (2010)(stating that "[t]he reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence. Debates rage over whether particular government information gathering activities invade 'privacy.'").

[166] Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920-21 (2005).

[167] 172 Cal. App. 4th 1125 (2009).

[168] *Id.* at 1130.

Under the judge's reasoning, had the plaintiff protected the website with a password, she might have had a reasonable expectation of privacy.[169] The judge failed to consider the other factors of obscurity. Was the poem visible to search engines? Did Moreno use her real name or an ID variant? Should theoretical accessibility be the *sine qua non* for rendering information public, thus denying it protection under privacy laws?

A useful conception of online obscurity could be helpful for these sorts of inquiries. Instead of an arbitrarily drawn line between public and private based on password use, courts could interpret where information fell on a spectrum of obscurity. Information subjected to all four factors that obviate obscurity would be deemed completely obvious, and thus undeserving of privacy protection. Information missing these elucidating factors would be deemed completely obscure, and most deserving of privacy protections. Of course, in the middle lies the grey area, where the information has at least one, but not all of the indicia of online obscurity. The law has developed methods to respond to other grey areas, such as fair use determinations. Thus, an analysis of online obscurity is not an insurmountable task.

To that end courts could ask the following questions based on the framework proposed in Part IV:

1. Was the information at issue able to be found via search engines?
2. Was access to the information restricted by password, biometrics, privacy settings or any other technology?
3. Was the information associated with an ID variant or pseudonym that is not easily traceable to a real identity, or was the identity of the discloser or subject of the information clear?
4. Was the information opaque to the extent that it was unlikely to be understood by unintended recipients?

By analyzing these factors independently at first, then as a whole, courts could come to a much more nuanced decision regarding whether to afford information privacy protections.

B. Obscurity as Protective Remedy

If online obscurity is conceptualized in a useful way, it need not be limited to a frame of analysis for courts. Obscurity could be a benefit conferred or middle ground between total secrecy and complete public disclosure. This is particularly true for information that might be embarrassing but not damaging enough to warrant the full force of robust privacy and confidentiality protections. In this way, obscurity could be a

[169] *Id.*

less effective, but also less costly remedy than complete confidentiality, anonymity, or "the right to be forgotten."[170] For example, courts seeking to balance privacy and access issues could hold that certain public records could remain online only if they receive certain obscurity protections.

In fact, courts and lawmakers are already offering obscurity as a procedural protection. They need only to expand the scope of its application. Courts and lawmakers have mandated the redaction of personal identifiers such as social security numbers from some public records.[171] Several of the proposed privacy protection laws focus on the collection of "personally identifiable information."[172] A new advocacy group, Without My Consent,[173] has advocated filing a lawsuit pseudonymously to respond to some invasions of privacy.[174] But these protections focus only on one aspect of obscurity – identification. As we have described, there are other ways to protect information with online obscurity.

Online obscurity could be seen as a double-edged sword. By embracing obscurity, courts and lawmakers could avoid traditional privacy protections such as sealed records and complete opacity by settling for obscurity. However, courts and lawmakers might also be willing to provide obscurity in situations where they were not willing to provide total secrecy or confidentiality. Obscurity could protect certain privacy interests while also promoting the dissemination of information. The FTC and other governmental agencies could consider obfuscation techniques as valid

[170] Ciaran Giles, *Internet 'Right to be Forgotten' Debate Hits Spain*, YAHOO! NEWS (Apr. 20, 2011), http://news.yahoo.com/s/ap/eu_internet_right_to_be_forgotten; VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2010).

[171] The E Government Act of 2002 instructed that personal identifiers, such as Social Security numbers and names of minor children should be redacted from federal court filings. Pub. L. No. 107-347, 116 Stat. 2899; 44 U.S.C. § 3501, et. seq. (2002); Peter W. Martin, *Online Access to Court Records—From Documents to Data, Particulars to Patterns*, 53 VILL. L. REV. 855 (2008) (stating that "the privacy concerns articulated in the E-Government Act led to a federal court policy and ultimately, effective December 1, 2007, new court rules directing attorneys to avoid the inclusion of certain personal identifying information (including full Social Security numbers) in case documents.").

[172] *See, e.g.*, Venkat Balasubramani, *A Look at the Commercial Privacy Bill of Rights Act of 2011*, TECHNOLOGY & MARKETING BLOG (Apr. 20, 2011), http://blog.ericgoldman.org/archives/2011/04/a_look_at_the_c.htm; Tanya Forsheit, *Breaking Down the Boucher Bill*, INFORMATION LAW GROUP (May 12, 2010), http://www.infolawgroup.com/2010/05/articles/behavioral-advertising/breaking-down-the-boucher-bill/.

[173] WITHOUT MY CONSENT, http://www.withoutmyconsent.org/ (last accessed April 27, 2011).

[174] *What Does It Mean to File a Lawsuit Under a Pseudonym?*, WITHOUT MY CONSENT, http://www.withoutmyconsent.org/home/will-the-court-let-me-file-a-lawsuit-as-plaintiff-jane-doe/ (last accessed April 27, 2011).

protections of certain kinds of consumer information or in certain contexts.[175]

Online information that is not searchable, accessible or understandable poses less of a threat to a user's privacy. By making information obscure online, the law could to curtail certain abuses of "big data" and perhaps effectuate some of the spirit of the OECD Privacy Guidelines.[176] Thus, obscurity could represent a compromise between those seeking to publish or access information and those seeking to restrict it. The proper distinction would then be between which pieces of information required confidentiality or secrecy and which pieces would be adequately protected with online obscurity.

The purpose of Section II of this article was to demonstrate that Internet users desire and rely upon the obscurity of some of their online information. Like any other desirable result, obscurity could be a benefit that is negotiated for both in legal disputes and commercial transactions. For instance, if an individual sues a website for public disclosure of private facts, a compromise could be having the website block a certain article from being searched instead of a complete deletion of information or a monetary settlement.[177] This would lower the likelihood information would be found by parties such as potential employers searching for information, but allow the website to keep the information posted.

Again, online obscurity as a protective measure would hardly be suitable for information likely to be shared and widely linked to throughout the Internet. Some information, particularly those concerning celebrities and public officials, must be kept a near secret or highly confidential to avoid being widely distributed on the Web. Additionally, it is very difficult to predict what information will go viral online. However, much information online is banal, uninteresting, or irrelevant to most people, but still potentially harmful to some users. Think of photos of a typical high school

[175] Commercial data brokers also collect obscure but available information online and could be regulated under this approach. *See, e.g.,* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection,* 2006 U. ILL. L. REV. 357 (2006).

[176] Org. for Econ. Co-operation and Dev., OECD Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data (2002), http:// www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (setting forth data privacy guidelines for industry and governments that enable the transborder transfer of information).

[177] Plaintiffs in privacy disputes having an increasingly difficult time collecting monetary damages. *See, e.g.,* Daniel Solove, *The Slow Demise of Defamation and Privacy Torts*, HUFFINGTON POST (Oct. 12, 2010, 11:14 am), http://www.huffingtonpost.com/daniel-j-solove/the-slow-demise-of-defama_b_758570.html.

student involving alcohol being viewed by college admissions counselors, potential employers and the like. Most people have no interest in viewing or incentive to look for these pictures. Obscurity could be most beneficial to those users who might be harmed by such information.

This socially irrelevant information is benign so long as it remains obscure, and is only likely to be harmful if it made obvious via one of the factors of online obscurity (search visibility, unrestricted accessibility, identification, and clarity). Consider the average job applicant. Many professionals have asserted that your online resume (what employers can quickly find about you online) is just as, if not more, important than your actual resume.[178]

However, not all information about online is likely to be found or read by employers – only the obvious (non-obscure) information is likely to be found. According to Michael Fertik and David Thompson, "Content that cannot be found by an average user in five minutes or less is not part of your online resume at all; for example, information about you that can be found only through a detailed query in a very specific government database might make up some part of your online reputation, but it is not part of your online resume."[179] Thus, if a job applicant is concerned about how a potentially embarrassing or private photo might affect her job prospects, it might be effective to simply bury it in obscurity to minimize the likelihood it would be found in a routine background search by a potential employer. In this way, obscurity can be effective simply by leaving information in a certain online context.

A number of groups have already entered the obscurity business. Reputation.com is a company that helps individuals protect their reputation through a variety of techniques, including making harmful information more obscure by suppressing search results.[180] Former Duke cancer researcher Anil Potti hired Online Reputation Manager, "a company that helps clients push down unfavorable content in search engine results. The effort has crowded out coverage of [a research] scandal and retraction notices on medical journals' websites."[181]

A full exploration of online obscurity as a benefit or protection is beyond the scope of this paper. The purpose of this section was merely to

[178] *See, e.g.,* MICHAEL FERTIK & DAVID THOMPSON, WILD WEST 2.0: HOW TO PROTECT AND RESTORE YOUR ONLINE REPUTATION ON THE UNTAMED SOCIAL FRONTIER 25 (2010).

[179] *Id.* at 26.

[180] *See* REPUTATION.COM, http://www.reputation.com/reputationdefender (last accessed April 15, 2011).

[181] Taylor Dohtery, *Potti Hires Online Reputation Manager*, THE CHRONICLE (Apr. 14, 2011) http://dukechronicle.com/article/potti-hires-online-reputation-manager.

propose how online obscurity might serve as a legal benefit or halfway point between two extremes of no protection and total secrecy.

C. Share Alike: An Agreement to Maintain Obscurity

Obscurity could also play a role in agreements concerning online information. The current discussion surrounding online agreements and privacy centers on confidentiality agreements and consent to obtain and use personal information.[182] Explicit confidentiality agreements are difficult to obtain for Internet users and are costly for the recipient of information.[183] By agreeing to keep information confidential, users are largely prohibited disclosing the confidential information at all.

If online obscurity is usefully conceptualized, then, in some instances, it could serve as an alternative to the standard confidentiality agreement. Instead of binding adherents to a duty of confidentiality, disclosers of information could require a duty to maintain obscurity. This could be done by refraining from supplying any or all of the factors that make information more obvious: (e.g. do not make information visible to search engines, keep information protected by privacy settings, do not associate names with the information, etc…).

This approach highlights online obscurity's reliance on Nissenbaum's theory. These agreements would essentially require recipients of information to keep the information as obscure as they found it. In other words, recipients would be bound to respect the information's contextual integrity. By identifying specific factors critical to online obscurity, adherents would have a clearer picture of the practices that would constitute breach of their agreement.

Agreements to maintain online obscurity could resemble the "share alike" principal embedded in Creative Commons and open software licenses. Creative Commons is an organization which offers a variety of copyright licenses that allow creators to choose the degree to which their

[182] *See, e.g.*, Allyson Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587 (2007); Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545 (2006); Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. L. REV. 529 (2007).

[183] *See, e.g.*, Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887 (2006); Nancy S. Kim, *'Wrap Contracts and Privacy*, Association for the Advancement of Artificial Intelligence Press Technical Report SS-10-05, 2010, at 1, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1580111 (last visited July 2, 2010); Sandra Braman & Stephanie Roberts, *Advantage ISP: Terms of Service as Media Law*, 5 NEW MEDIA & SOCIETY 422 (2003); Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 460 (2006).

work can be utilized and the terms on which it can be shared.[184] Under their "share alike" provision, copyright owners license others to do things like remix, tweak, and build upon the work in a non-commercial way, as long as user of the work licenses their new creations under the identical terms stipulated by the original copyright owner.[185] Following the share alike principle, adherents to obscurity agreements would simply keep the information as generally obscure as they found it.

Promises to maintain obscurity might be most relevant when new technology in introduced in established contexts. Consider facial-recognition technology and social media. When uploading photos to social network sites or sharing sites like Facebook and Flikr, users are often promised that the website will respect both the user's privacy and their privacy settings.[186] An important function of some of these websites is the ability to tag photos.[187] Once a photo is tagged with an identifier, such as a name or link to a profile, it becomes searchable. According to our conceptualization, making information visible to search significantly erodes the protection of obscurity, and, consequently, threatens a user's privacy. Thus, if a website promised to respect a user's privacy and privacy settings, a destruction of online obscurity could be seen as a breach of that promise.

User-website agreements are not the only kind of agreements that could incorporate online obscurity. Agreements between Internet users could also involve a duty to refrain from making information more obvious. Instead of binding users to an agreement of confidentiality, Internet users interacting with each other, for example in online communities, could also promise to keep the information as obscure as they found it. In this way, it would advance Lior Strahilivetz's social networks theory of privacy.[188] Obscurity could be an effective way to implement that theory. Social networks are difficult to define, but users might have an easier time respecting specific obfuscation techniques. It is largely clear how to refrain

[184] *About*, CREATIVE COMMONS, http://creativecommons.org/about (last accessed April 29, 2011).

[185] *About the Licenses*, CREATIVE COMMONS, http://creativecommons.org/licenses/ (last accessed April 29, 2011).

[186] *See, e.g.*, Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. (forthcoming 2011).

[187] *See, e.g., What is Photo Tagging?*, FACEBOOK, https://www.facebook.com/help/?faq=13407 (last accessed April 29, 2011); *Search and Locate: Tagging photos*, PICASA, http://picasa.google.com/support/bin/answer.py?answer=106209 (last accessed April 29, 2011); *Posting*, TUMBLR, http://www.tumblr.com/docs/en/posting (last accessed April 29, 2011)(discussing how to tag posts).

[188] Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920-21 (2005).

from making information searchable or freely accessible, rather than attempt to guess the limits of these "blurry-edged networks."[189]

As with the previous potential applications of online obscurity, a full explication of a potential duty to maintain obscurity is beyond the scope of this article and will be addressed in future research. The purpose of this section was to illuminate how agreements regarding personal information can encompass more than just duties of confidentiality. A duty to maintain obscurity could be a desirable and manageable goal for parties entering into an agreement regarding personal information.

CONCLUSION

In Aldous Huxley's novel *Those Barren Leaves,* one of the main characters, Mrs. Thriplow, conversed with a houseguest on the difficulty of being genuine in the face significant public exposure.[190] She stated, "I get quite frightened when I see my name in the papers and photographers want to take pictures of me and people ask me out to dinner. I'm afraid of losing my obscurity. Genuineness only thrives in the dark. Like celery."[191] Mrs. Thriplow's fears echo the concerns of those who disclose information online. Perhaps more than anything else, Internet users rely on obscurity for protection of their online information. This obscurity allows Internet users to be genuine by disclosing information that they would not otherwise share in "public." Yet this concept, which is at the very heart of the social Web, is largely undeveloped in privacy law.

In this paper, we have attempted to make the case for obscurity online. While obscurity, and being obscure, is an everyday phenomenon, it is important to understand that we bring our practices of obscurity online as well. As our online and offline networks interact, and online environments move away from anonymity and pseudonymity to "nonymity," we have created and evolved a rich set of strategies to protect our disclosures online. Collectively, we describe these strategies as producing obscurity, a flexible strategy for the management of disclosure in increasingly heterogenous, nonymous environments.

We have argued that the reason the law has failed to embrace online obscurity is because the concept lacks a coherent meaning. To that end, we have offered the first conceptualization of online obscurity as a doctrinal model. Information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We have identified four of these factors as part of a non-exhaustive list: 1) search

[189] *See,* Gelman, *supra* note 1.
[190] ALDOUS HUXLEY, THOSE BARREN LEAVES 13 (1925).
[191] *Id.*

visibility, 2) unprotected access, 3) identification, and 4) clarity. The presence of these factors diminishes obscurity, and their absence enhances it. Thus, in determining whether information is obscure online, courts should consider whether any of these factors were present in their determination. Information that is entirely un-obscure is completely obvious, and vice versa. Courts should engage in a case-by-case analysis of the factors, examining each one individually, then as a whole to determine the degree of online obscurity.

This article also proposed ways that conceptualization could be implemented to remedy the tension between privacy law and the expectations of Internet users. This framework could be applied in numerous online privacy disputes as an analytical tool or as part of an obligation. Obscurity could be relied upon as a continuum when courts are asked to determine if information is eligible for privacy protections. Obscurity could be used as a benefit or protection – instead of forcing websites to remove information, a compromise could be some form of mandated obscurity. Finally, obscurity could serve as a metric for the boundary of allowable disclosure by information recipients. Internet users who were bound to a “duty to maintain obscurity” would be allowed to further disclose information, so long as they kept the information as generally obscure as they received it.

This conceptualization and proposed implementations of online obscurity are meant to be introductions, not the final word. Much more research and analysis is required to fully explore how online obscurity might be utilized by the law. As researchers have pointed out, the emergence of the nonymous social Web introduces challenges to traditional models of studying online identity and disclosure. We must update our understanding of information sharing in these environments, with both observational and inferential analysis. In doing so, we will better understand how individuals shift their expectations of obscurity offline to these increasingly populated and important online environments.

Courts and lawmakers can no longer allow online obscurity to languish in privacy doctrine. The concept is too central to the expectations of Internet users. Instead, online obscurity should be embraced as a useful concept capable of alleviating the problems associated with flawed approaches like the public/private dichotomy. Online obscurity could be another useful tool to address the array of privacy problems in the digital age, but only if it is pulled from the shadows.

***