2013

The Case for Online Obscurity

Woodrow Hartzog
Boston University School of Law

Frederic Stutzman

California Law Review

VOL. 101 FEBRUARY 2013 NO. 1

The Case for Online Obscurity

Woodrow Hartzog* & Frederic Stutzman**

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, and therefore ineligible for privacy

* Assistant Professor of Law, Cumberland School of Law at Samford University; Affiliate Scholar, Center for Internet and Society at Stanford Law School.

** Visiting Assistant Professor, School of Information and Library Science, University of North Carolina at Chapel Hill.

The authors would like to thank Alessandro Acquisti, Gaia Bernstein, Will DeVries, Tony Fargo, Lauren Gelman, Joe Hall, Chris Hoofnagle, Airi Lampinen, William McGeveran, Helen Nissenbaum, Neil Richards, Sasha Romanosky, Daniel Solove, the Future of Privacy Forum, the faculty at H. John Heinz III College at Carnegie Mellon University, Samford University's Cumberland School of Law, and the University of North Carolina at Chapel Hill and the participants of workshops hosted by Microsoft Research New England, the CYLAB Usable Privacy and Security Lab, the Privacy Law Scholars Conference, the Yale Information Society Project, and the International Association of Privacy Professionals. This research was generously funded by the Cumberland School of Law, the Roy H. Park Fellowship, the Margaret E. Kalp Fellowship and the IWT SBO Project on Security and Privacy for Online Social Networks (SPION).

protection. Drawing from multiple disciplines, this Article develops a more focused, clear, and workable definition of online obscurity: information is obscure online if it lacks 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. Viewing obscurity as a continuum could help courts and lawmakers determine if information is eligible for privacy protections. Obscurity could also serve as a compromise protective remedy: instead of forcing websites to remove sensitive information, courts could mandate some form of obscurity. Finally, obscurity could form part of an agreement where 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.

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 almost reflexively on the obscurity created by

these techniques to protect their privacy in daily life.[1] 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] "newsworthiness,"[3] and the "reasonable expectation of privacy."[4] However, "obscurity" has yet to have a clear legal conceptualization or role. 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 better defining online obscurity, this Article aims to provide a framework that is more effective than the current approach to 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,[5] or insider knowledge.[6] Other pieces of online information are obfuscated by the

---

1. *See, e.g.*, danah boyd, *Why Youth ♥ Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 133 (David Buckingham ed., 2008), *available at* 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."); Danielle Keats 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 Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1317–18 (2009); James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1160–63 (2009). This assertion is addressed in greater detail in Part II.

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

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

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

5. *See* Memorandum from Berners-Lee et al., Network Working Group Members of the Internet Engineering Task Force, to the Public for Comments on RFC 1738: Uniform Resource Locators (URL) (Dec. 1994), *available at* http://www.ietf.org/rfc/rfc1738.txt. A URL, or Uniform Resource Locator, describes "syntax and semantics of formalized information for location and access of resources via the Internet." *Id.* For example, the web address http://yahoo.com is a URL that resolves to the Yahoo website.

6. *See, e.g.*, Michael K. Bergman, *The Deep Web: Surfacing Hidden Value*, 7 J. ELECTRIC PUBLISHING, http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.

use of pseudonyms, multiple profiles, and privacy settings.[7] 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.[8]

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 accessible by anyone in possession of the URL? If a website introduces searchable facial recognition technology, has it broken any promises of privacy to users who previously uploaded photos and may have relied on the fact those photos were not previously searchable?

Drawing upon empirical research from multiple disciplines, this Article develops a focused, clear, and workable definition of online obscurity: information is obscure online if it lacks 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 to online privacy disputes in various ways. Courts could use an obscurity continuum when determining if certain information is eligible for privacy protections. Obscurity also could be used as a protective remedy—instead of forcing websites to remove information, courts and lawmakers could, in appropriate contexts, mandate a form of obscurity. Finally, obscurity could replace confidentiality as a term in some contracts. Internet users bound by 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.

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."); Norm Medeiros, *Reap What You Sow: Harvesting the Deep Web*, 18 OCLC SYS. & SERVS. 18 (2002); Yanbo Ru & Ellis Horowitz, *Indexing the Invisible Web: A Survey*, 29 ONLINE INFO. REV. 249 (2005); Danny Devriendt, *Data Is Gold – 91,000 Terabytes of Uncharted Web: Welcome to the Dark Side*, PORTER NOVELLI BLOG (Apr. 11, 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."); Russell Kay, *Quickstudy: Deep Web*, COMPUTERWORLD (Dec. 19, 2005, 12:00 PM), 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."); *see also* PAUL PEDLEY, THE INVISIBLE WEB: SEARCHING THE HIDDEN PARTS OF THE INTERNET (2001); CHRIS SHERMAN & GARY PRICE, THE INVISIBLE WEB: UNCOVERING INFORMATION SOURCES SEARCH ENGINES CAN'T SEE (2001).

7. *See, e.g.*, boyd, *supra* note 1, at 133; Frederic Stutzman & Woodrow Hartzog, Boundary Regulation in Social Media, *in* PROCEEDINGS OF THE ACM 2012 CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK 769, 769–78 (2012), *available at* http://dl.acm.org/citation.cfm?id=2145320&bnc=1.

8. *See infra* Part III.

Part I of this Article explores the general concept of obscurity and the vital role it plays in our everyday lives. Part II identifies the tactics and strategies individuals employ to obscure themselves in online settings. Part III 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

The American Heritage Dictionary defines obscure as "Not readily noticed or seen; inconspicuous; . . . Not clearly understood or expressed; ambiguous or vague."[9] We operationalize obscurity as a simple concept, reflecting of *a state of unknowing*. In the context of interpersonal relations, what does it mean for an individual to be obscure? Obscurity at the individual level involves two parties: the individual and the observer. An individual is obscure to an observer if the observer does not possess or comprehend critical information needed to make sense *of* the individual. Personal identity, social connections, and personal or situational context are examples of such critical information. Without this information, the observer has a limited 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. This "zone of obscurity" protects individuals from identification while facilitating social interaction.

We argue the case for obscurity for two reasons. First, we argue that obscurity is a common and natural condition of interaction, and therefore human expectation of obscurity will transfer to the domains in which we spend time, both physical and virtual. Second, we argue that obscurity is a desirable state because we are protected by an observer's inability to comprehend our actions, and therefore social practice encourages us to seek obscurity. To make these arguments, we explore the cognitive and cultural logic of obscurity, focusing particularly on evolutionary biologist Robin Dunbar's analysis of cognitive economy and how it produces obscurity, and sociologist Erving Goffman's analysis of interaction and how we enact obscurity in everyday life. With this analysis, we demonstrate that obscurity is both a physically essential state and one that is culturally recognized as desirable. We are then able to extend our analysis to online settings, where obscurity is commonplace.

9. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 1213 (4th ed. 2000), *available at* http://www.ahdictionary.com/word/search.html?q=obscure (defining "obscure").

In arguing that obscurity is commonplace, we draw on Dunbar's work to illustrate the cognitive logic of obscurity. Dunbar's work on the "Social Brain Hypothesis" famously demonstrated that human cognitive groups—clusters of individuals that have shared communication, memories, and interpersonal relationships—are fairly small, with a maximum group size of approximately 150 members.[10] Dunbar was careful to draw a distinction between simply identifying and truly knowing people, pointing out that we can recognize about 2000 people, far more than the maximum number of people knowable at the individual level.[11] The Social Brain Hypothesis illustrates the evolutionary logic of a limited cognitive group: to prevent the overburdening of memory, we necessarily limit our cognitive groups to a manageable size.[12] Accordingly, most interactions outside of our cognitive groups occur in states of obscurity.

Viktor Mayer-Schönberger has extended this logic, highlighting work that demonstrates that forgetting is a cognitive advantage.[13] Our memories are purposefully selective to prevent cognitive overburdening.[14] This realistically means that most of the individuals with whom we interact in passing, or share common space in transit, are obscure to us and we to them—they are strangers. Furthermore, obscurity in interactions with strangers produces notable effects, such as conversational freedom.[15] Most of us live a day-to-day existence where we are only close to a few individuals.[16] Genetic disposition toward obscurity is therefore reinforced by everyday practice.

It is important not to conflate lack of personal identification with anonymity. In everyday life, people identify others at varying personal and social levels, such as through appearance, role or position, or ritual activity.[17]

---

10. *See, e.g.*, R.I.M. Dunbar, *Coevolution of Neocortical Size, Group Size and Language in Humans*, 16 BEHAV. & BRAIN SCI. 681 (1993); R.I.M. Dunbar & M. Spoors, *Social Networks, Support Cliques, and Kinship*, 6 HUM. NATURE 273 (1995).

11. Robin I.M. Dunbar, *The Social Brain Hypothesis*, 6 EVOLUTIONARY ANTHROPOLOGY 178, 184 (1998).

12. *Id.* at 184.

13. *See* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 16–49 (2009) (explaining why remembering is more resource intensive than forgetting).

14. *Id.* at 17–18.

15. John A. Bargh et al., *Can You See the Real Me? Activation and Expression of the "True Self" on the Internet*, 58 J. SOC. ISSUES 33, 44–45 (2002).

16. There is some debate over measuring the size of human social groups, but even those debating measurement methodology agree that the average number of people to whom one is truly close—and nonobscure—to remains objectively small. *See* LEE RAINIE & BARRY WELLMAN, NETWORKED: THE NEW SOCIAL OPERATING SYSTEM 117–34 (2012) (discussing measurement of personal networks, effects of online interaction on personal networks); Miller McPherson et al., *Social Isolation in America: Changes in Core Discussion Networks over Two Decades*, 71 AM. SOC. REV. 353, 360 (2006) (establishing and updating core discussion network size). Notable exceptions to this claim are celebrities or other highly identifiable individuals. *See* GRAEME TURNER, UNDERSTANDING CELEBRITY 23–26, 46–51 (2004).

17. SUSAN T. FISKE & SHELLEY E. TAYLOR, SOCIAL COGNITION (2d ed. 1991); John M. Levine et al., *Social Foundations of Cognition*, 44 ANN. REV. PSYCHOL. 585, 592 (1993) (explaining

For example, we are able to construct a set of expectations about 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 an individual's social behavior deviates from the norm or expectation.[18] Indeed, the possibility of being identified tends to foster behavior that conforms to social norms, a concept familiar to anyone who has been exhorted to behave a certain way because "you never know who is watching." Therefore, humans produce obscurity by employing a range of strategies to increase the odds that their actions or bodies cannot be fully comprehended (in some cases) or identified (in others). Thus, it is important to explore how and why obscurity is produced in everyday life.

As Goffman argues, processes of identification and comprehension are a function of the range of signals we give off both purposefully and accidentally.[19] Our dress and demeanor convey "front-stage" signals—those we intend our observers to draw upon as they make sense of our actions.[20] 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.[21] For example, an individual effectuating a certain dialect may momentarily slip up, unintentionally revealing information about social class or background.[22] According to Goffman, our ability to "read" a scene, and thus appropriately judge how we present ourselves, is a critical component in social interaction.[23] We utilize a range of cues and physical structures to figure out how we should present ourselves.[24] For example, our understanding of the private nature of a conversation is moderated by the presence of walls and

---

how some observers expect certain individuals to behave a certain way based on the "social position" the observer perceives the individual to be in).

18. In off-line settings, individuals may seek personal information to explain observed deviant behavior, such as finding out the backstory 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 et al., *Social Identification and Interpersonal Communication in Computer-Mediated Communication: What You Do Versus Who You Are in Virtual Groups*, 35 HUM. COMM. RES. 59, 64–65 (2009).

19. ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 17–21 (1959).

20. *Id.* at 22–30.

21. *Id.* at 111–22.

22. *Id.* at 39–47.

23. 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.

Erving Goffman, *Felicity's Condition*, 89 AM. J. SOC. 1, 51 (1983).

24. *See* ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES: NOTES ON THE SOCIAL ORGANIZATION OF GATHERINGS 151–65 (1963).

doors.[25] These physical structures provide privacy and feature into the overall structure and content of interpersonal interaction; we often say things behind a closed door that we would not say in public.[26]

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 an accent may actually be using obscurity offensively to create an unrealistic impression, whereas another individual may cloak herself or himself in obscurity to prevent informational 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.[27]

Obscurity is a biological and social process—one that is culturally and cognitively embedded and reinforced through social interaction. The next Section shows how our expectations of obscurity off-line impact our privacy decisions online and how the practice of obscurity is enacted online, where geography, identity presentation, and physical structure are different.

II.
THE PRODUCTION OF ONLINE OBSCURITY

When deciding to share information online, an individual follows implicit and explicit rules, cultural norms, prior attitudes, expectations, and desired outcomes.[28] As is the case off-line, the choice to disclose information online is the product of a complex and highly contextual decision process, where risks are weighed against the potential rewards resulting from disclosure.[29] As illustrated in the preceding Section, people expect obscurity in everyday life; it is the product of physical, social, and cognitive processes.[30] Extending this logic, we argue that obscurity is assumed, expected, and actively produced in

25. *Id.*

26. *Id.*

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

28. *See, e.g.*, Adam N. Joinson & Carina B. Paine, *Self-Disclosure, Privacy and the Internet*, *in* THE OXFORD HANDBOOK OF INTERNET PSYCHOLOGY 237, 237–38 (Adam N. Joinson et al. eds., 2007); Rob Kling et al., *Assessing Anonymous Communication on the Internet: Policy Deliberations*, 15 INFO. SOC'Y 79, 82–84 (1999); Su-Yu Zeng et al., *Sharing Private Information Online: The Mediator Effect of Social Exchange*, *in* PROCEEDINGS OF THE 11TH INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE 231 (2009), *available at* http://dl.acm.org/ft_gateway.cfm?id=1593290&ftid=652035&dwn=1&CFID=194561741&CFTOKEN=39062883.

29. *See* Leysia Palen & Paul Dourish, *Unpacking "Privacy" for a Networked World*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 129, 131–33 (2003), *available at* http://dl.acm.org/citation.cfm?id=642635&bnc=1 (discussing the tensions between privacy and publicity).

30. *See supra* Part I.

online settings. Internet use is now so widespread that differences between users and nonusers are largely attributable to socioeconomic or geographic differences, as opposed to behavioral or attitudinal ones.[31] Online obscurity is a general expectation, and not the sole purview of a certain class of Internet user.

What does it mean to expect obscurity online? Empirical evidence shows that individual use of the Internet is influenced by, and reflective of, existing cognitive schemas.[32] That is, our identities, expectations, roles, and norms will often transfer to online settings.[33] 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 reinforce off-line social structures.[34] Furthermore, although a number of legal opinions suggest otherwise, empirical evidence demonstrates that individual use of the Internet does not necessarily indicate the seeking of a wide audience.[35] A person should not expect fame or notoriety simply because she or he uses the Internet. Multiple studies of user attention and audience online have revealed a "long tail" distribution of attention online—the majority of attention online is

31. *See, e.g.*, SUSANNAH FOX, PEW INTERNET & AM. LIFE PROJECT, DIGITAL DIVISIONS: THERE ARE CLEAR DIFFERENCES AMONG THOSE WITH BROADBAND CONNECTIONS, DIAL-UP CONNECTIONS, AND NO CONNECTIONS AT ALL TO THE INTERNET (2005), *available at* http://www.pewinternet.org/PPF/r/165/report_display.asp; JOHN HORRIGAN, PEW INTERNET & AM. LIFE PROJECT, HOME BROADBAND ADOPTION 2009 (2009), *available at* http://www.pewinternet.org/Reports/2009/10-Home-Broadband-Adoption-2009.aspx. As these reports clearly indicate, use and nonuse of Internet resources is largely a function of socioeconomic 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. *See, e.g.*, KATHRYN ZICKUHR & AARON SMITH, PEW INTERNET & AM. LIFE PROJECT, DIGITAL DIFFERENCES (2012), *available at* http://pewinternet.org/Reports/2012/Digital-differences.aspx (noting that nonusers primary reasons involved lack of motivation, access to resources, or difficulty in use). We speculate that while use or nonuse of the Internet is poorly explained by privacy preferences, use and nonuse of certain applications may be better explained by privacy preference.

32. *See* RAINIE & WELLMAN, *supra* note 16, at 126–31; Andreas Wimmer & Kevin Lewis, *Beyond and Below Racial Homophily: ERG Models of a Friendship Network Documented on Facebook*, 116 AM. J. SOC., 583, 588–600 (explaining the theoretical bases for racial homogeneity in social networks).

33. *See* Wimmer & Lewis, *supra* note 32.

34. The reinforcement of social structure can be broadly categorized into two frames. The first frame involves the replication of material and socioeconomic conditions and practices in online space, which is often conceived of as the digital divide. *See, e.g.*, KAREN MOSSBERGER ET AL., VIRTUAL INEQUALITY: BEYOND THE DIGITAL DIVIDE, 1–15, 60–73 (2003); Ritu Agarwal et al., *Social Interactions and the "Digital Divide": Explaining Variations in Internet Use*, 20 INFO. SYS. RES. 277, 277–94 (connecting internet use with peer behavior and social influence); Eszter Hargittai, *Digital Na(t)ives? Variation in Internet Skills and Uses Among Members of the "Net Generation,"* 80 SOC. INQUIRY 92, 108 (2010) (concluding that differences in web-use skills correlate with socioeconomic, racial, and gender differences). The second frame is the replication of off-line network structures online; that is, the degree to which online and off-line networks overlap, inherently forcing individuals to fall into off-line social roles. *See, e.g.*, RAINIE & WELLMAN, *supra* note 16, at 126–30 (discussing the "diminishing" gap between physical space and cyberspace); Wimmer & Lewis, *supra* note 32, at 588–600 (discussing the important role off-line social structure exerts on online network formation).

35. *See infra* Part III.

dedicated to a small number of producers, with the majority of content producers having small audiences.[36]

While cognitive models of online participation are influenced by off-line schemas, important differences remain between the two. Rob Kling et al. discuss two major structural differences in online and off-line communication in their analysis of online anonymity.[37] First, online discussion is amenable to "mass dissemination," as messages posted online can be transmitted much faster than through traditional means.[38] Second, messages posted online have "persistence," in that messages can be replicated, archived, and essentially made permanent through cheap digital copies.[39] Similarly, social media scholar danah boyd describes the four primary components of networked publics, or digital public spheres for socio-technical interaction: persistence, searchability, replicability, and invisibility of audiences.[40] The core logic of boyd's persistence and replicability components mirrors Kling et al.'s discussion of persistence and mass dissemination, so they are not discussed at length here. 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.[41] There is no parallel in off-line space, boyd argues—no universal mechanism that allows instantaneous searching through all possible geographies.[42] The term "invisible audiences" refers to the state of unknowing that is common in online disclosure.[43] When sharing a post or tweet online, we have a general idea who will see our content, but we cannot know if our message will be seen by unanticipated audiences. Compare this to the off-line equivalent: when we disclose in public, we generally have an idea of who the entire audience is, even if we do not actually know the audience. Because disclosures online are persistent, people have a hard time predicting where these disclosures will go, or who will see them, further incentivizing Internet users to seek online obscurity.[44]

The challenge faced by users of Internet technologies when managing personal disclosure online is the pressure to act within socially constructed

36. *See, e.g.*, Andrei Broder et al., *Graph Structure in the Web*, 33 COMPUTER NETWORKS 309 (2000); Jon M. Kleinberg, *Authoritative Sources in a Hyperlinked Environment*, 46 J. ACM 604 (1999). For an applied discussion of attention networks in Twitter, see Meeyoung Cha et al., *Measuring User Influence in Twitter: The Million Follower Fallacy*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL AAAI CONFERENCE ON WEBLOGS AND SOCIAL MEDIA 10 (2010), *available at* http://www.aaai.org/ocs/index.php/ICWSM/ICWSM10/paper/view/1538/1826.

37. Kling et al., *supra* note 28, at 87.

38. *See id*.

39. *See id*.

40. boyd, *supra* note 1, at 120, 126.

41. *Id.* at 120.

42. *Id.*

43. *Id.*

44. *Id.* at 126, 131–34. For example, consider the case of Aleksy Vayner, whose video resume "Impossible Is Nothing" became an Internet meme. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 171–78 (2007).

rules of interpersonal disclosure, which draw strongly on off-line norms, while also managing privacy and disclosure goals in light of key structural differences in the online environment. The rise of social media, perhaps surprisingly, indicates our expectation of obscurity online and illustrates how obscurity is more important than ever for managing online disclosures. In the following Sections, we explore the practice of online obscurity. We demonstrate that people seek and expect online obscurity as they do off-line 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[45] have resulted in dramatic increases in online participation and sharing. According to the Pew Internet and American Life Project, nearly 75 percent of all adults use the Internet, and virtually all teens aged twelve to seventeen (93 percent) are Internet users.[46] 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*.[47] This shift towards identity-centric content is dramatic, and has serious implications for both privacy and identity online. Shanyang Zhao et al. 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

45. *See, e.g.*, BLOGGER, http://www.blogger.com/ (last visited Nov. 10, 2012); FACEBOOK, https://www.facebook.com/ (last visited Nov. 10, 2012); FOURSQUARE, https://foursquare.com/ (last visited Nov. 10, 2012); TWITTER, https://twitter.com/ (last visited Nov. 10, 2012); WORDPRESS.COM, http://wordpress.com/ (last visited Nov. 10, 2012).

46. *See, e.g.*, AMANDA LENHART, PEW INTERNET & AM. LIFE PROJECT, ADULTS AND SOCIAL NETWORK WEBSITES (2009), *available at* http://www.pewinternet.org/PPF/r/272/report_display.aspx; AMANDA LENHART & MARY MADDEN, PEW INTERNET & AM. LIFE PROJECT, TEENS, PRIVACY AND ONLINE SOCIAL NETWORKS (2007), *available at* http://www.pewinternet.org/PPF/r/211/report_display.asp; AMANDA LENHART ET AL., PEW INTERNET & AM. LIFE PROJECT, SOCIAL MEDIA AND YOUNG ADULTS (2010), *available at* http://pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

47. Shanyang Zhao et al., *Identity Construction on Facebook: Digital Empowerment in Anchored Relationships*, 24 COMPUTERS HUM. BEHAV. 1816, 1818–19 (2008) (citations omitted).

> 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.[48]

As Zhao et al. note, the shift from anonymous to nonymous communication in online settings poses 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 or deindividuated communication settings.[49] Second, there is a relatively novel overlap between nonymous mediated communication settings and off-line settings.[50] With the growth of peer-produced content, we are increasingly communicating nonymously online with the same people with whom we interact off-line.[51] For this reason, privacy management in nonymous online communication requires the management of overlaps and boundaries in off-line networks—if a person wishes to communicate nonymously yet maintain control over disclosures, she or he must develop strategies that permit selective or targeted disclosures. In the following Section, we review literature that identifies some of these techniques of managed disclosure. In doing so, we demonstrate that the practice of obscurity is useful for communicating in variably nonymous environments.

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 heterogeneous—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.[52] How do individuals manage privacy and disclosure, and the goals and outcomes associated with sharing in the network, as audiences shift? Joan M. DiMicco and David R. Millen described a vivid example of inherent network diversification as

48. *Id.*

49. *See, e.g.*, NANCY BAYM, PERSONAL CONNECTIONS IN THE DIGITAL AGE 50–58 (2010).

50. *See* RAINIE & WELLMAN, *supra* note 16, at 126–30.

51. Cliff Lampe et al., *A Face(Book) in the Crowd: Social Searching vs. Social Browsing*, *in* CSCW '06 PROCEEDINGS OF THE 2006 20TH ANNIVERSARY CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK 167 (2006), *available at* http://dl.acm.org/citation.cfm?id=1180901&bnc=1 (discussing the online network construction of college students). For a more general discussion of online-off-line overlaps, see, for example, RAINIE & WELLMAN, *supra* note 16, at 126–30.

52. DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD 15–17, 275 (2010).

students move from college to their first job at a technology firm.[53] Using surveys, the authors developed social network site profile "types" identifying a simple and highly functional disclosure management strategy.[54] In particular, DiMicco and Millen found that people at different levels of the organizational structure operate differently in social media, with adoption and disclosure levels negatively correlating with organizational embeddedness.[55] Individuals that were more strongly embedded in the network (i.e., more senior) were more likely to have limited profiles and to limit disclosures.

DiMicco and Millen's study was conducted in 2007, and adoption of Facebook was not as broad based then as it is today.[56] Later work conducted by Meredith M. Skeels and Jonathan Grudin[57] 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 site.[58] One particular source of tension is the family network and family interactions with work networks.[59] In establishing friendships across social hierarchies, individuals are required to maintain a coherent identity across these hierarchies—a significant challenge.[60] Airi Lampinen et al. documented strategies individuals use to manage identity across network boundaries.[61] The authors describe the use of both behavioral and mental strategies for boundary management.[62] Behavioral strategies include using social network sites selectively (e.g., maintaining a "personal" and "business" account) or "self-censoring" certain types of content.[63] Examples of mental strategies include developing interpersonal arrangements

53. Joan Morris DiMicco & David R. Millen, *Identity Management: Multiple Presentations of Self in Facebook*, *in* GROUP '07: PROCEEDINGS OF THE 2007 INTERNATIONAL ACM CONFERENCE ON SUPPORTING GROUP WORK 383 (2007), *available at* http://dl.acm.org/citation.cfm?id=1316682.

54. *Id.* at 384.

55. *See id.* at 384–86.

56. *See* KIRKPATRICK, *supra* note 52, at 16, 275.

57. Meredith M. Skeels & Jonathan Grudin, *When Social Networks Cross Boundaries: A Case Study of Workplace Use of Facebook and LinkedIn*, *in* GROUP '09: PROCEEDINGS OF THE ACM 2009 INTERNATIONAL CONFERENCE ON SUPPORTING GROUP WORK 95 (2009), *available at* http://dl.acm.org/citation.cfm?id=1531689.

58. *Id.* at 100–01.

59. *Id.* at 96, 100–01.

60. *Id.* at 102–03.

61. Airi Lampinen et al., *All My People Right Here, Right Now: Management of Group Co-presence on a Social Networking Site*, *in* GROUP '09: PROCEEDINGS OF THE ACM 2009 INTERNATIONAL CONFERENCE ON SUPPORTING GROUP WORK 281 (2009) [hereinafter Lampinen et al., *All My People*], *available at* http://dl.acm.org/citation.cfm?id=1531717; Airi Lampinen et al., *We're in It Together: Interpersonal Management of Disclosure in Social Network Services*, *in* CHI '11: PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2011), *available at* http://dl.acm.org/citation.cfm?id=1979420.

62. Lampinen et al., *All My People, supra* note 61, at 287.

63. *Id.* at 287–89.

to manage disclosure or specifying trust relations around certain types of disclosures.[64]

As we have argued, the selective management of identity is a natural and commonly occurring phenomenon, and individuals have been managing their identities online since before the rise of social media. The use of simple obfuscation techniques, such as pseudonyms,[65] confidentiality agreements, relational (in-group) knowledge, and techniques of true anonymity (such as encryption) have been long accessible to users of Internet technology.[66] Kuanchin Chen and Alan I. Rea extended this analysis, identifying three primary types of techniques used by online participants to manage identity disclosures.[67] First is the falsification of information shared online, which involves techniques such as using multiple email accounts, deleting cookies, and lying to websites.[68] Second is passive reaction, which involves the use (or destruction) of technology that would connect a person to his or her online footprints.[69] Third is identity modification, which involves the creation of gender-neutral avatar names, and the use of online identities that are disassociated from the personal identity.[70] 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, particularly the nonymous social web. When an individual faces censure from her or his peer group for lying publicly, or 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.

We argue that a lack of access to existing identity protection techniques is not a tacit dismissal of their value but a catalyst for creativity. Individuals do not abandon their desire for privacy; rather, they seek privacy in contextually appropriate ways. Consider "mirror networks," one of the earliest documented "innovations" in privacy and disclosure control to emerge from social media.[71] Teenage users of social media sites increasingly faced the specter of surveillance from parents and other individuals of authority.[72] Rather than withdrawing from social network sites, the teenagers created densely

64. *Id.* For example, individuals might agree "how far" interpersonal disclosures should travel (i.e., whether they should be kept secret, shared only with close friends, or disclosed to everyone).

65. *See, e.g.*, Houn-Gee Chen et al., *Online Privacy Control Via Anonymity and Pseudonym: Cross-cultural Implications*, 27 BEHAV. & INFO. TECH. 229 (2008).

66. *See, e.g.*, Kling et al., *supra* note 28, at 81–82.

67. Kuanchin Chen & Alan I. Rea, Jr., *Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques*, 44 J. COMPUTER INFO. SYS. 85, 87–88 (2004).

68. *Id.* at 90.

69. *Id.* Chen and Rea provide examples such as deleting unnecessary accounts or ignoring contact or email requests. *Id.* at 90.

70. *Id.*

71. boyd, *supra* note 1, at 132.

72. *Id.* at 131–34.

interconnected mirror profiles—highly sanitized copies of the profile that were densely connected within the personal friend network.[73] In essence, these profiles created an alternate reality where parents could snoop, and teenagers enjoyed privacy in completely separate, hidden zones of obscurity.[74]

The authors' own empirical research has explored the privacy practices of social media users, focusing particularly on those that used multiple profiles as an identity management strategy.[75] In a similar vein to the work of Lampinen and colleagues, this research explored the challenges of, and reaction to, increasingly heterogeneous disclosure networks within social media.[76] Maintaining multiple profiles within social network sites represents an active "segmentation" of the site into multiple zones of obscurity.[77] Most commonly, social networks are segmented along important network boundaries such as family, work, and public persona.[78] Depending on the importance of the linkage between these personas, individuals use various techniques to "cloak" personas, such as employing privacy settings, using obscure name variants, and highly regulating the off-line disclosure of the existence of the profile.[79]

The use of multiple profiles represents an innovative approach to the challenges of disclosure within the platform, but it also represents a fundamental failing of the platform to respect disclosure and privacy intent. Work by Heather Richter Lipford et al. attempted to rectify this through the design of technologies that adaptively match privacy intent to disclosure goals in social network sites.[80] In particular, Lipford et al. drew on Helen Nissenbaum's notion of contextual integrity[81] as a metaphor for system design.[82] If users are given control over disclosures, they may be better able to

73. *Id.* at 132.

74. 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 the nature of the communication. This renders the networks practically "hidden" from existing techniques that could be employed to discover them, particularly text search. *Id.*

75. Stutzman & Hartzog, *supra* note 7.

76. *Id.* at 771–72.

77. *Id.* at 775–76.

78. *Id.* at 773–76.

79. *Id.* at 772–73.

80. *See, e.g.*, Andrew Besmer & Heather Richter Lipford, *Moving Beyond Untagging: Photo Privacy in a Tagged World, in* CHI '10: PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1563 (2010), *available at* http://dl.acm.org/citation.cfm?id=1753560; Heather Richter Lipford et al., *Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites*, *in* 4 CSE '09 PROCEEDINGS OF THE 2009 INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE AND ENGINEERING 985 (2009), *available at* http://dl.acm.org/citation.cfm?id=1633633; Katherine Strater & Heather Richter Lipford, *Strategies and Struggles with Privacy in an Online Social Networking Community*, *in* 1 BCS-HCI '08 PROCEEDINGS OF THE 22ND BRITISH HCI GROUP ANNUAL CONFERENCE ON PEOPLE AND COMPUTERS: CULTURE, CREATIVITY, INTERACTION 111 (2008), *available at* http://dl.acm.org/citation.cfm?id=1531530.

81. *See infra* Part III.

82. Lipford et al., *supra* note 80, at 985–86.

share information in accordance with their goals and desires, and they will not have to react reflexively to systems and algorithms.[83]

Although social media is often thought of as a public, nonymous space, we have demonstrated that individuals employ a range of practices to manage and optimize their privacy. In particular, individuals exert control over the information they disclose by limiting the audience of the disclosure, by bounding the meaning of the disclosure, and by reflexively adapting the disclosure to the site. In social media, where anonymity often violates social norms or site terms, 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 their expectation of privacy and obscurity.

A powerful popular discourse argues that individuals have essentially different privacy and notoriety goals online than they do off-line.[84] It is therefore essential that we provide evidence that obscurity online is socially expected and desired. The previous two Sections have attempted to demonstrate that online obscurity is a crucial aspect of privacy for Internet users. As we have demonstrated, obscurity is both expected and desired online. The next Part discusses how, even though obscurity is a central aspect of online privacy, the concept is languishing in privacy law.

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.[85] 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 appears implicit in a number of disputes, courts seem to wrap it into larger or different concepts

83. *Id.* at 987–89. For example, Facebook would have respected user privacy and avoided a user revolt if users were able to "opt in" to the Facebook newsfeed. *See* KIRKPATRICK, *supra* note 52, at 189–95.

84. *See, e.g.*, Emily Nussbaum, *Say Everything*, N.Y. MAG., Feb. 12, 2007, at 24–29, 102–03, *available at* http://nymag.com/news/features/27341/.

85. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 104–26 (2010) [hereinafter NISSENBAUM, PRIVACY IN CONTEXT]; DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1–37 (2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY]; Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) [hereinafter Nissenbaum, *Privacy as Contextual Integrity*]; Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998) [hereinafter Nissenbaum, *Protecting Privacy in an Information Age*]; Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) [hereinafter Solove, *Conceptualizing Privacy*]; Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

of privacy law, such as "public" information.[86] Although courts and scholars have approached the disconnect between law and individual notions of privacy from a number of angles, many conflicts seem to stem from one problem—individuals have complex notions of privacy in regard to personal information but the law tends to treat that information only two ways: public or private.[87] This maligned on/off approach to privacy has been called the "public-private dichotomy"[88] or "secrecy paradigm."[89]

Although this dichotomy has distorted the societal expectations of privacy before the Internet, it has proven to be even more unworkable online. This Part highlights the failure of courts and lawmakers to embrace online obscurity. The need for a workable concept of online obscurity is as important as determining what constitutes "public" online information. This Part will first review the public/private dichotomy in privacy law and critics' arguments as to why it is flawed. This Part will then explore case law concerning online disclosure. While these cases show that courts have failed to adequately consider obscurity in analyzing whether information is public, they also suggest that courts might be willing to embrace an obscurity paradigm. Finally, this Part will examine statutes and regulations that implicitly value obscurity as a means to protect privacy but fail to adequately conceptualize obscurity.

A. The Public/Private Dichotomy

Daniel Solove describes the "secrecy paradigm" as an understanding of privacy based on concealment preventing others from invading one's hidden world.[90] Under this conception, disclosed information is no longer concealed and, thus, no longer private.[91] Sharon Sandeen noted that this vision of privacy "makes it difficult for individuals to protect personal information once it has been shared with others."[92] Solove argued that the secrecy paradigm "fails to

86. *See, e.g.*, United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002), *rev'd on other grounds*, 90 F. App'x 3 (1st Cir. 2004); Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 44 (Minn. Ct. App. 2009).

87. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1177 (2002) (noting that when privacy is equated with secrecy, "[i]nformation is categorized as either public or private. . . . Understood this way, information has a particular status; it can either be in one domain or another. The law often treats information in this black-and-white manner; either it is wholly private or wholly public.").

88. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 85, at 113–25; Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 85, at 136.

89. Solove, *supra* note 87, at 42.

90. *Id.*

91. *Id.*

92. Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 694. Online obscurity has also appeared in the trade secret literature. *See, e.g.*, Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1, 17–19 (2007). Rowe asked the question of trade secret doctrine: "Does public mean public accessibility or public publication? Does the obscurity of the

recognize that individuals want to keep things private from some people but not others."[93] The concept of obscurity can play a key role in addressing the issues that the secrecy paradigm overlooks.

Disclosing information to some, but not all, is difficult in modern society. Solove asserts 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.[94]

Solove recognizes the utility of obscurity. Regarding doctrinal notions of "public," Solove claims 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."[95] 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 posits 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."[96]

Helen Nissenbaum argues that the public/private dichotomy fails to consider context, which rationalizes an individual's desire to have "privacy in public."[97] 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."[98] 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

---

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.*

93. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 43–44 (2004).

94. *Id.* at 44; *see also infra* Parts I and II.

95. SOLOVE, *supra* note 93, at 44.

96. Solove, *Conceptualizing Privacy*, *supra* note 85, at 1152.

97. Nissenbaum, *Protecting Privacy in an Information Age*, *supra* note 85, at 559 n.2. *See also* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 85; Helen Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 85.

98. Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 85, at 132.

> 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."[99]

In essence, information that falls within the private half of the public/private dichotomy warrants privacy consideration; "for all the rest, anything goes."[100]

Nissenbaum also rejects the public/private distinction in law. Instead, she proposes 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.'"[101] 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."[102]The integrity of these contexts is preserved when norms of appropriateness and the flow of information are maintained, and this maintenance of contextual norms is the hallmark of privacy.[103] As will be discussed in Part 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.[104] Dianne Zimmerman explains that "[t]o 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."[105] Courts using the subject matter analysis "rule that the subject matter is private even though the locus is not."[106]

---

99. *Id.* at 135–36 (emphasis omitted).
100. *Id.* at 136–37.
101. *Id.* at 137 (emphasis omitted).
102. *Id.* at 137.
103. *Id.* at 138.
104. *See, e.g.*, 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); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291 (1983).
105. Zimmerman, *supra* note 104, at 347.
106. *Id.* at 348.

Zimmerman found that both approaches are practically unfeasible and threaten freedom of speech.[107]

Not all scholars have found the public/private dichotomy problematic. Heidi Reamer Anderson defines obscurity simply as "the absence of exposure."[108] Anderson defends the public/private dichotomy as beneficial to resolving the "obscurity problem," which occurs when a private actor lawfully collects and further exposes information that someone else initially shared in public.[109] 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 research that demonstrates the significant role obscurity plays in the disclosure of information online. As demonstrated in Part II of this Article, obscurity is not simply an incidental 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 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 and contexts 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

107. *Id.* at 344–50.

108. Heidi Reamer Anderson, *The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 551 (2012).

109. *Id.* at 550–51. Anderson ultimately concludes that "a potential loss in obscurity is a small price to pay for . . . [the benefits gained from transparency], and that the 'no privacy in public' rule generally remains valid." *Id.* at 602.

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 to rely on 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 off-line impediments to data retrieval, was articulated by the Supreme Court in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*.[110] In evaluating the privacy of a "rap sheet" containing aggregated public records, the Supreme Court 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.[111] The information was considered practically obscure because of the extremely high cost and low likelihood of the information being compiled by the public.[112] Thus, practical obscurity became a recognized, yet undeveloped, concept in privacy doctrine. The doctrine has largely been confined to disputes involving access to public records,[113] computer security,[114] and governmental searches.[115] Beyond a general sense

---

110. 489 U.S. 749, 770 (1989).

111. *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.

112. *Id.* at 764, 780.

113. *See, e.g.*, 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."); Lewis A. Kaplan, *Litigation, Privacy and the Electronic Age*, 4 YALE SYMP. ON L. & TECH 1, ¶ 6 (2001) ("This practical obscurity of information generated in all but the most exceptional cases has been eroded by technological advances."); 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); Peter A. Winn, *Judicial Information Management in an Electronic Age: Old Standards, New Challenges*, 3 FED. CTS. L. REV. 135 (2009); 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 (2005); 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).

114. 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

that shared or available information does not always constitute public information, courts have had a difficult time expanding upon the concept.[116]

Doctrinal support for practical obscurity forms the foundation for utilizing the concept of obscurity in online disputes.[117] In *Burnett v. County of Bergen*,[118] 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

anonymized identities, in order to design responses that protect identity even in this worst case."); *cf.* Peter P. 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.").

115. A few have advocated online obscurity in the context of governmental searches. *See, e.g.*, David A. 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* 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."); Matthew J. 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.").

116. A number of scholars have argued that the traditional notion of practical obscurity, which relied on off-line impediments to discovery, no longer exists in a digital world. *See, e.g.*, Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1100–01 (2002) ("[W]hile the scattering of information throughout numerous computer databases had preserved some practical obscurity, the Internet has all but eliminated those remnants of isolation."); 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."); Omar Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1440 ("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 . . . .").

117. *See, e.g.*, *In re* French v. Am. Gen. Fin. Servs., 401 B.R. 295 (Bankr. E.D. Tenn. 2009); Finnerty v. State Bank & Trust Co., 687 S.E.2d 842 (Ga. Ct. App. 2009); Burnett v. Cnty. of Bergen, 968 A.2d 1151 (N.J. 2009); Lambert v. Hartmann, 898 N.E.2d 67 (Ohio Ct. App. 2008).

118. 968 A.2d at 1154.

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."[119]

The court cited *Reporters 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."[120] The court went on to say that "composite documents—in this case records that would be made available in a searchable computer database—implicate privacy concerns much more broadly than documents with one item alone."[121]

This same principle compelled the Supreme Court of Michigan in *Michigan Federation of Teachers v. University of Michigan*[122] to conclude that university employees' home addresses and telephone numbers were protected by the Michigan Freedom of Information Act'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 interest 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.[123]

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."[124] 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 off-line limitations to accessing information, courts have been

---

119. *Id.* at 1164.

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

121. *Id.*

122. 753 N.W.2d 28 (Mich. 2008).

123. *Id.* at 42 (quoting U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 500 (1994)).

124. *Id.*

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

> [i]t 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.[125]

In *J.S. v. Bethlehem School District*, the Commonwealth Court of Pennsylvania stated,

> [T]he 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.[126]

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, protecting their website with a password, and delisting their website from search engines with robot.txt files.[127] As will be 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 analyses of the concept to technological restrictions like passwords.

3. "Unlimited" Access

Courts typically presume that online information is "public" if anyone can find and access it, thereby ignoring any concept of obscurity.[128] A good

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

126. J.S. v. Bethlehem Area Sch. Dist., 757 A.2d 412, 425 (Pa. Commw. Ct. 2000).

127. *See* Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65.

128. *See, e.g.*, Boring v. Google, Inc., 362 F. App'x 273 (3d Cir. 2010); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) ("Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."); Sandler v. Calcagni, 565 F. Supp. 2d 184 (D. Me. 2008); United States v. D'Andrea, 497 F. Supp. 2d 117 (D. Mass. 2007); Four Navy Seals v. Associated Press, 413 F. Supp. 2d 1136 (S.D. Cal. 2005); United States v. Gines-Perez, 214 F. Supp. 2d 205 (D.P.R. 2002); Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862–63 (Ct. App. 2009); Yath v. Fairview Clinics, 767 N.W.2d 34 (Minn. Ct. App. 2009); State v. Birchfield, No. 04-08-00132, 2007 WL 1437235 (N.J. Super. Ct. App. Div. May 17, 2007).

example of this tendency is *United States v. Gines-Perez*.[129] In *Gines-Perez*, the U.S. District Court for Puerto Rico considered whether the use of a photograph that police downloaded from a website violated the defendant's right to privacy.[130] The defendant claimed that the police obtained the downloaded picture from a "private" website.[131] 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.[132]

The court found that the defendant had no subjective or reasonable expectation of privacy in the photographs posted online.[133] 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 page is 'under construction.'"[134] The court noted that the intention of the communicator in posting information online is irrelevant.[135] 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."[136]

Regarding the reasonableness of a claim to privacy, the court in *Gines-Perez* found that 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."[137] Despite its earlier declaration that the intent of the discloser was 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 the Defendant

129. 214 F. Supp. 2d at 225.

130. *Id.* at 224.

131. *Id.*

132. *Id.*

133. *Id*. at 225. The "reasonable expectation of privacy" test is a complex and often maligned doctrine requiring analysis beyond the scope of this Article. It is sufficient for the purposes of this Article to acknowledge that courts generally hold that individuals do not have a reasonable expectation of privacy in "public" information for Fourth Amendment purposes. *See* Donald R.C. Pongrace, *Stereotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 AM. U. L. REV. 1191, 1196, 1206–11 (1985). For more information, see, for example, 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); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511 (2010); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077 (1987).

134. *Gines-Perez*, 214 F. Supp. 2d at 225.

135. *Id.*

136. *Id.*

137. *Id.*

did not employ protective measures or devices that would have controlled access to the Web page or photograph itself."[138] As we argued in Part II, empirical research demonstrates that users do not intend to renounce privacy rights when posting on the Internet. Yet the type of analysis employed in *Gines-Perez* persists.

For example, in *Sandler v. Calcagni*, 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.[139] In *State v. Birchfield*, the Superior Court of New Jersey held that the "defendant had 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."[140]

Finally, in *Four Navy Seals v. Associated Press*, the U.S. District Court for the Southern District of California considered whether military personnel had a reasonable expectation of privacy in website photos that a journalist found via a search engine.[141] The journalist accessed and downloaded these photos "without the necessity of keying in any password, entering a code or incurring a monetary charge."[142] The court found that the journalist's "act of downloading photos from a publicly-accessible website . . . was not an egregious breach of social norms underlying the state privacy right."[143] Rather, it found that "one cannot reasonably expect the [I]nternet posting of photos to be private."[144]

As we will discuss, search visibility is a critical component of online privacy but courts should not consider availability of information as the sole factor in their analyses. Barriers to access, such as passwords, codes, and monetary charges, are also effective and forceful tools for the creation and maintenance of online obscurity. However, these barriers—particularly passwords—often seem to be the only obscurity factor that courts consider. The following cases demonstrate how courts have recognized that restricted websites might be considered private under various thresholds, even though completely unprotected websites are ineligible for privacy protection. Yet, without a definition of online obscurity, the cases reveal that courts are likely to end their analyses after considering barriers to access such as passwords and encryption.[145] This refusal to consider other factors of obscurity has seemingly

138. *Id.*
139. 565 F. Supp. 2d 184, 197 (D. Me. 2008).
140. No. 04-08-00132, 2007 WL 1437235, at *3 (N.J. Super. Ct. App. Div. May 17, 2007).
141. 413 F. Supp. 2d 1136 (S.D. Cal. 2005).
142. *Id.* at 1141.
143. *Id.* at 1143.
144. *Id.* at 1147.
145. However, a few courts have looked beyond passwords. See *Four Navy Seals v. Associated Press*, 413 F. Supp. 2d 1136, 1145 (S.D. Cal. 2005), and *J.S. v. Bethlehem Area School District*, 757 A.2d 412, 425 (Pa. Commw. Ct. 2000), for a discussion on search visibility.

resulted in the unspoken general rule that password-restricted disclosures are private, while all other disclosures online are public.

The mentality that websites with no access barriers are "public" is reflected in courts' opinions. The court in *Gines-Perez* enunciated the importance of protective measures in creating a reasonable expectation of privacy. The court admitted 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**."[146] In *Pietrylo v. Hillstone Restaurant Group*, 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.[147] An employee at a local restaurant created a group to vent about his employer "without any outside eyes spying in on [them]."[148] The website creator stated that "[t]his group is entirely private, and can only be joined by invitation."[149] The court noted that the icon for the group, which was the restaurant's trademarked logo, "would appear only on the My[S]pace profiles of those who were invited into the group and accepted the invitation."[150]

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.[151] The court found that the "[p]laintiffs created an invitation-only [I]nternet discussion space. In this space, they had an expectation that only invited users would be able to read the discussion."[152]

By giving such weight to password protections, *Pietrylo* laid the foundation for a concrete concept of obscurity. In *United States v. D'Andrea*,[153] 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."[154] 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

146. United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) (emphasis in original).
147. No. 06-5754, 2008 WL 6085437 (D.N.J. July 25, 2008).
148. *Id.* at *1.
149. *Id.*
150. *Id.*
151. *Id.* at *1–2.
152. *Id.* at *6.
153. 497 F. Supp. 2d 117 (D. Mass. 2007).
154. Couillard, *supra* note 115, at 2225 (emphasis omitted).

to claim a reasonable expectation of privacy in the site's contents."[155] LaFave asserted that "[r]eliance 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."[156]

In *Kelleher v. City of Reading*, the U.S. District Court for the Eastern District of Pennsylvania also noted the importance of passwords in affording a reasonable expectation of privacy. The court concluded that "an employee might have a reasonable expectation of privacy in certain e-mail communications, depending upon the circumstances of the communication and the configuration of the e-mail system"[157]—seemingly an allusion to password protection. The U.S. Court of Appeals for the Armed Forces supported privacy in emails protected by passwords in *United States v. Long*, stating, "[W]e find that the password [protection] . . . support[s] the lower court's conclusion that Appellee met her burden of demonstrating a subjective expectation of privacy."[158] The focus on the importance of password protection in *D'Andrea*, *Kelleher*, and *Long* suggests that courts are willing to depart from the rule that individuals have no expectation of privacy in information posted online. Because of this willingness to protect information that is shared only with some users, courts may be receptive to the concept of online obscurity as privacy protection.

Several courts have considered barriers to access other than passwords in determining whether online information deserves privacy protection. These courts found it relevant to consider whether a computer shared its files or its access to a network in determining if the information on a computer was "public."[159] In *United States v. Stults*, the U.S. Court of 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."[160] The court drew an analogy to an off-line situation, stating, "One who gives his house keys to all of his friends who request them should not be surprised should one of them open

155. *D'Andrea*, 497 F. Supp. 2d at 121.

156. *Id.* (citing WAYNE R. LAFAVE, 1 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f) at 721 (4th ed. 2004)).

157. No. CIV. A. 01-3386, 2001 WL 1132401, at *5 (E.D. Pa. Sept. 24, 2001).

158. 64 M.J. 57, 63 (C.A.A.F. 2006).

159. *See, e.g.*, United States v. Durdley, No. 1:09–cr–00031–MP–AK, 2010 WL 916107, at *4–5 (N.D. Fla. Mar. 11, 2010) (citing United States v. King, 509 F.3d 1338 (11th Cir. 2007) (finding that the accidental sharing of files over a computer network and thumb drive left in a common use computer destroyed a reasonable expectation of privacy)); Interscope Records v. Duty, No. 05CV3744-PHX-FJM, 2006 WL 988086, at *3 (D. Ariz. Apr. 14, 2006) ("[I]t is undisputed that the share[d] file is publically available, therefore [the counterclaimant] cannot show that the Recording Companies intruded upon her private affairs [by accessing the file-sharing folder on her computer].").

160. 575 F.3d 834, 843 (2009).

the door without knocking."[161] 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."[162]

The U.S. District Court for the District of Oregon reached a similar conclusion in *United States v. Ahrndt*, finding that an unsecured wireless network and an iTunes folder configured to share access with any surrounding computers utilizing the same software defeated a claim for a reasonable expectation of privacy.[163] 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.

While most courts have only looked at barriers to access to determine whether online information is public, some courts have considered whether a website containing the information can be located via a search engine. 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 [I]nternet, and used no deception in locating and downloading the images."[164] In *J.S. v. Bethlehem Area School District*,[165] the Commonwealth Court of Pennsylvania ruled that a student maintained no reasonable expectation of privacy in a website he created because the website was not password-protected.[166] According to the court, "any user who happened upon the correct search terms could have stumbled upon [the] [s]tudent's web-site. For example, a search of the terms 'Bethlehem Area School District' may have found [the] [s]tudent's site in its results."[167] This focus on search visibility adds a layer to the public/private analysis and cuts against the secrecy paradigm's central tenet that disclosed information is no longer private. Instead, search visibility focuses on contextual factors and the reality of how individuals find information and communicate online. Courts should further utilize this factor. 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.

Judicial recognition of practical obscurity, as well as courts' willingness to find privacy protection in the use of passwords and other access barriers, suggest that courts are ready to embrace the concept of online obscurity. Until the law provides a workable framework for obscurity in the context of online

161. *Id.*
162. *Id.* (citations omitted).
163. No. 08-468-KI, 2010 WL 373994, at *3–9 (D. Or. Jan. 28, 2010).
164. Four Navy Seals v. Associated Press, 413 F. Supp. 2d 1136, 1145 (S.D. Cal. 2005).
165. 757 A.2d 412, 425 (Pa. Commw. Ct. 2000).
166. *Id.* (explaining that a protected website would mean that "only certain viewers could access the site by use of a known password").
167. *Id.*

privacy, however, judges will continue to stand by the general rule that information posted on a website accessible to anyone is "public" information.

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 instead clarified 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 prohibits the disclosure of certain information about any individual obtained by the DMV in a motor vehicle record.[168] Of course, much of the information protected by this statute, such as home address and appearance, is hardly secret, or even private. But by restricting access to this information, the law implicitly protects whatever obscurity the information exists in. A similar logic applies to the Video Privacy Protection Act, which prohibits videotape service providers from disclosing information such as an individual's rental history.[169] Other videotape shoppers might be able to observe an individual renting a particular movie in public, but that information would be unknown to the public at large. This law therefore supports obscurity.

Financial and commercial privacy laws also restrict the disclosure of "personal information" or "personally identifiable information," which, while often private, sometimes includes information that is not seen as a secret.[170] A recent dispute resulted in a determination that even a zip code qualified as

168. 18 U.S.C. §§ 2721–2725 (2006). The Act defines "personal information" as "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address, . . . telephone number, and medical or disability information . . . ." 18 U.S.C. § 2725(3).

169. 18 U.S.C. § 2710 (2006). It should be noted that the Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2013), arguably weakened the statute's privacy protections by allowing video tape service providers to use advance consent obtained over the Internet to justify the disclosure of consumers' personally identifiable information. *See, e.g.*, Chloe Albanesius, *Obama Signs Bill That Lets You Share Netflix Activity on Facebook*, PCMAG.COM (Jan. 11, 2013, 4:11 PM), http://www.pcmag.com/article2/0,2817,2414206,00.asp; John Paul Titlow, *Thanks Congress, but We Need Privacy Laws, Not Banal Social Sharing*, READWRITE (Dec. 26, 2012), http://readwrite.com/2012/05/09/sites-with-social-reading-apps-sacrifice-readers-to-facebook.

170. *See, e.g.*, Massachusetts Breach Notification Statute, 201 MASS. CODE REGS. § 17.01 (2009) (defining "personal information" as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account"); California Data Security Breach Statute, CAL. CIV. CODE § 1798.81.5 (2004).

protected information.[171] Critics of this decision failed to see how a zip code could be private.[172] This critique suggests that the court's use of the term "privacy" in this case might be more confusing than clarifying. 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 treatment of this topic is beyond the scope of this Article and has been well addressed by others.[173] However, if legislatures attempt to address privacy issues involving "public" information online, we suggest that in some instances it is not privacy generally, but obscurity specifically, that such laws should support or protect.

In sum, courts and lawmakers have not explicitly embraced online obscurity, although the concept is implicit in the resolution of several privacy disputes. Obscurity has been derided as misguided[174] or ineffective in actually addressing privacy concerns,[175] but these labels are often unfair and inaccurate when applied to online information. As discussed in Part II, obscurity is a

---

171. *See* Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612, 619–20 (Cal. 2011); Bob Egelko, *Stores That Request ZIP Codes Violate Law*, S.F. CHRON., Feb. 11, 2011, at D1.

172. *See, e.g.*, Kashmir Hill, *A Ridiculous California Court Ruling: Zip Codes Are Private*, FORBES (Feb. 11, 2011, 12:52 PM), 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 (TAP) (Mar. 8, 2011), http://www.techpolicy.com/PinedaLaw-of-Jungle_Hoofnagle.aspx (arguing that the *Pineda* decision restrains "commercial actors that have no respect whatsoever for consumer preferences" from collecting personal information).

173. *See, e.g.*, NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 85; SOLOVE, UNDERSTANDING PRIVACY, *supra* note 85.

174. *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, 1024 (2002) ("[T]he *Reporters Committee* 'central purpose' definition and theory of 'practical obscurity' are judicial inventions aimed at ill-defined concerns . . . .").

175. *See, e.g.*, Richard J. Peltz et al., *The Arkansas Proposal on Access to Court Records: Upgrading the Common Law with Electronic Freedom of Information Norms*, 59 ARK. L. REV. 555, 636 (2006) (stating that *Reporters 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 *Reporters 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.

Jane E. Kirtley, *The EU Data Protection Directive and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639, 642 (1995); Bepko, *supra* note 113, at 984 ("But is a privacy right threatened when a compilation of otherwise hard to find information—what is now available in the courthouse—is disclosed on the Internet? . . . [I]t does not follow that access to information alone is necessarily harmful.").

crucial component of online privacy. However, the utility of online obscurity is entirely dependent upon a useful conceptualization and manageable framework.

IV.
PROPOSED DEFINITION AND FRAMEWORK FOR ONLINE OBSCURITY

Recall the dictionary definition of obscurity as "Not readily noticed or seen; inconspicuous; . . . Not clearly understood or expressed; ambiguous or vague."[176] This understanding of obscurity provides a helpful starting point in the attempt 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.[177] 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 that impede the understanding or discovery of information.[178] Given the ease of aggregation and the irrelevance of physical space online, little meaning can be extracted from the concept underlying practical obscurity. As previously discussed, online obscurity is concerned not with geographic or physical burdens, but rather with different kinds of obfuscation.[179]

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: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity. This definition draws upon the previously detailed theoretical and empirical research and requires some explication.

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.[180] The theory of privacy as contextual integrity proposes that privacy violations occur when the

176. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE, *supra* note 9, at 1213 (defining "obscure").

177. *See, e.g.*, SOLOVE, UNDERSTANDING PRIVACY, *supra* note 85, at 1–2.

178. *See supra* notes 113–15 and accompanying text.

179. *Cf.* Finn Brunton & Helen Nissenbaum, *Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation*, 16 FIRST MONDAY (May 2, 2011), http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3493/2955 (developing a political philosophy of obfuscation where actors produce "misleading, false, or ambiguous data with the intention of confusing an adversary or simply adding to the time or cost of separating bad data from good."). We think the proper metaphor for online obscurity is the key and lock. The key and lock metaphor is well suited to online disputes given the judicial reliance on the digital version of the key: the password. In essence, we simply propose that there is more than one key that can lock information. Indeed, many kinds of keys and locks, each with varying strengths, exist. Considered cumulatively, these metaphorical keys and locks fall along a spectrum that will allow courts to make a more nuanced analysis of online information based on a scale of obscurity.

180. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 85; Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 85; Nissenbaum, *Protecting Privacy in an Information Age*, *supra* note 85.

disclosure of one individual's personal information by another disrespects the context in which the information is disclosed.[181]

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)."[182] Nissenbaum claims that these norms, which she refers 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."[183] Nissenbaum explains that context-relative informational norms are simultaneously reflections of expectations of privacy in certain contexts and vehicles for prescribing ways to evaluate or respond to potential threats to privacy.[184]

Nissenbaum defines context as "structured social settings with characteristics that have evolved over time . . . and are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more."[185] A central tenet of contextual integrity provides that "there are no arenas of 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."[186] Because Nissenbaum's theory focuses on context, it is well suited to frame our approach to online obscurity, which is almost entirely context-dependent.

Our conceptualization of online obscurity also draws upon Lior Strahilevitz's "Social Networks Theory of Privacy," which 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 network.[187] Strahilevitz explains how tort law typically analyzes expectations of privacy, stating, "If it is theoretically possible, but extraordinarily unlikely, that information shared with a few individuals will ultimately become widely known by the public, then privacy tort law usually discounts the theoretical possibility and holds that the data privacy subject maintains a reasonable expectation of privacy."[188]

---

181. Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 85, at 141.

182. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 85, at 3.

183. *Id.*

184. *Id.* at 129.

185. *Id.* at 130.

186. Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 85, at 137 (emphasis omitted).

187. Strahilevitz, *supra* note 85, at 920–21, 972, 988.

188. Lior Jacob Strahilevitz, *Reunifying Privacy Law,* 98 CALIF. L. REV. 2007, 2039 (2010) [hereinafter Strahilevitz, *Reunifying Privacy Law*] ("As I explained in *A Social Networks Theory of Privacy*, tort law typically analyzes expectations of privacy through a probabilistic lens."). Therefore, an individual who minimizes the likelihood that the public will discover her information generally enjoys a reasonable expectation of privacy. *Cf.* Lior Jacob Strahilevitz, *Pseudonymous Litigation,* 77

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. In defining obscurity as the product of an analysis of the critical four factors, we enable flexible application of the framework across domains. Whereas technologists may wish to weigh the factors of search visibility or unprotected access more highly in application, policy makers may place more weight on anonymity and clarity. We purposefully do not weigh factors; while we realize that the framework factors will vary in importance based on setting and context, we allow individuals to determine this balance according to the situation.

For example, 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 off-line and online are significant enough to require a conceptualization of obscurity contoured to the online 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 evaluating all information on the Internet.

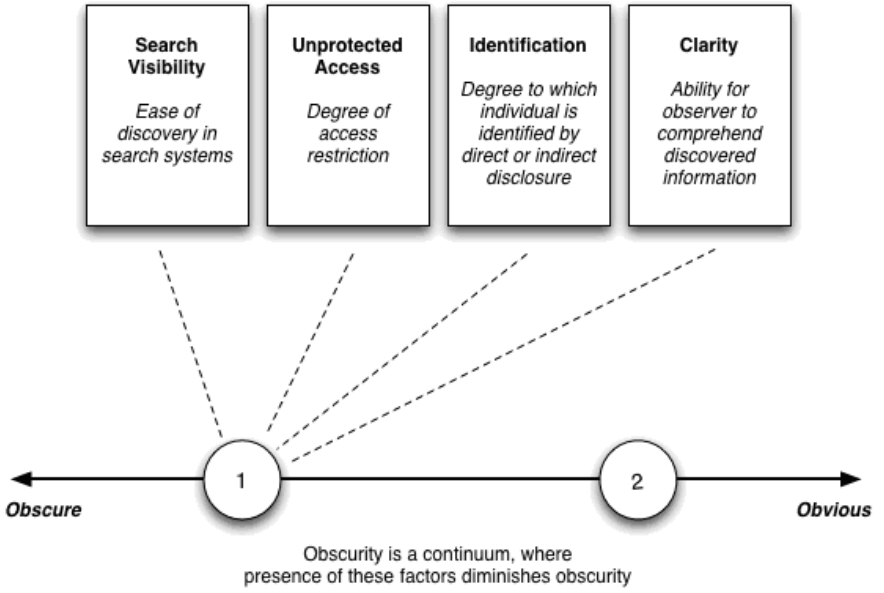
To reiterate, information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We adopt the dictionary definition for discovery, which is "the process of learning something that was not known before, or of finding someone or something that was missing or hidden."[189] We define comprehension as the ability to understand the information in a given context.

As already noted, we have identified four of these key factors: (1) search 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. Information that is entirely unobscure 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. Figure 1 depicts how this conceptualization would work in two different scenarios.

U. CHI. L. REV. 1239, 1257–59 (2010) [hereinafter Strahilevitz, *Pseudonymous Litigation*] (describing the importance of using pseudonyms for one or both parties in certain disputes).

189. *Discovery Definition*, MACMILLAN DICTIONARY, http://www.macmillandictionary.com/dictionary/british/discovery (last visited Nov. 10, 2012).

FIGURE 1: Factors determining online 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 and understanding information: search visibility and unprotected access.[190] 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 one of the most significant factors in online obscurity. Search is the primary method for discovering online information, which is a key factor in our definition of obscurity.[191] Without search, individuals can discover information only in a chain-hyperlink fashion via other websites, messages, and manual URL entries.

190. Note that this is similar to the MySpace group formed in *Pietrylo v. Hillstone*, No. 06-5754, 2008 WL 6085437 (D.N.J. July 25, 2008). *See supra* note 147 and accompanying text.

191. *See, e.g.*, DEBORAH FALLOWS, PEW INTERNET & AM. LIFE PROJECT, SEARCH ENGINE USE 1 (2008), *available at* http://www.pewinternet.org/Reports/2008/Search-Engine-Use/Data-Memo.aspx; SUSANNAH FOX, PEW INTERNET & AM. LIFE PROJECT, SEARCH ENGINES 1 (2002), *available at* http://www.pewinternet.org/Reports/2002/Search-Engines/Data-Memo.aspx; LEE RAINIE,

Yet, most online information is not visible to search engines. This information, collectively known as "the dark Web,"[192] "the deep Web,"[193] or "the invisible Web,"[194] accounts for 80–99 percent of the World Wide Web.[195] The dark Web does not just consist of websites that programmers have intentionally shielded from search engines using the robot.txt file.[196] It also includes websites that use privacy settings or are behind access restrictions such as passwords, which are another factor in online obscurity.[197]

Thus, anyone applying the concept of online obscurity should give significant weight to search visibility. A finding that information can be discovered via search renders the information more obvious and thus less likely to be classified as private information. Information invisible to search, on the other hand, is more obscure and accordingly more likely to receive the benefit of privacy protections.

The breadth of the search visibility also matters. Information that is searchable at the site level is quite different from information searchable by the major Internet search engines (like Google or Bing) or by the deep-Web search engines (like Pipl and iSearch). Accordingly, information that is visible to searches of the entire Internet or can be located by a large number of search engines is more obvious and less obscure.

In addition to the breadth of search visibility, 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.[198] These and other mitigating factors will be addressed in future research.

PEW INTERNET & AM. LIFE PROJECT, BIG JUMP IN SEARCH ENGINE USE 1 (2005), *available at* http://www.pewinternet.org/Reports/2005/Big-jump-in-search-engine-use/Data-Memo.aspx; Gary Marchionini, *Exploratory Search: From Finding to Understanding*, 49 COMM. ACM 41 (2006).

192. *See* Devriendt, *supra* note 6.

193. *See* Bergman, *supra* note 6; Kay, *supra* note 6.

194. *See* Medeiros, *supra* note 6; Ru & Horowitz, *supra* note 6.

195. *See* Bergman, *supra* note 6; Devriendt, *supra* note 6; Kay, *supra* note 6; Ru & Horowitz, *supra* note 6.

196. *See, e.g.*, Zittrain, *supra* note 127, at 102 ("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.").

197. For example, the popular blogging service Blogger allows users to make their blog invisible to Google. *See "Listing" and "Let Search Engines Find Your Blog" Settings*, GOOGLE BLOGGER, http://www.google.com/support/blogger/bin/answer.py?hl=en&answer=41373 (last visited Nov. 10, 2012). Similarly, Facebook profiles that utilize privacy settings are also not found by search engines. *See 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 visited Nov. 10, 2012).

198. For example, finding information via search engines on a particular person with a common name such as "John Smith" would likely require additional search terms or iterative searches.

B. Unprotected Access

As discussed in Part III, in determining whether information is private, courts predominantly consider whether access to information is either unfettered or somehow restricted by technological features such as passwords and privacy settings.[199] While not dispositive, this approach is a significant part of the obscurity calculus. Not only does restricted access help prevent the discovery of information by unauthorized parties, it can also serve as an indicator of the private nature of the information to those with the right credentials.[200] Thus, barriers to access can also serve to communicate a desire or expectation of confidentiality as well as create obscurity.

Conversely, the lack of restrictions on information access, particularly when restrictions are available but unused, has the opposite effect on obscurity. A finding that information is accessible without restriction makes information less obscure and more obvious. Information protected by passwords, privacy settings, and the like is much more obscure, making it more likely to receive the benefit of privacy protections.

Like search, the scope of the restriction matters. Some access restrictions, like biometrics, encryption, and to a lesser degree, passwords, often offer more than obscurity—they offer means to protect secrets. However, privacy settings are a relatively new technology and do not yet completely reflect the users' wishes.[201] Also, as service providers change defaults and redefine fundamental concepts of privacy within their services, privacy settings will also shift. Thus, privacy measures should be analyzed on a case-by-case basis according to how restrictive they are or can be.

The number of people with access to information is also important in evaluating the breadth of the restriction. 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 granting access to "friends of friends" or everyone living in a general area. As computing systems evolve and adoption of privacy protections increases, we will see moves toward dynamically generated privacy zones—privacy that is reactive to the environment and network configurations within the

199. 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, 7:55 AM), http://www.computerworld.com/s/article/9206998/How_Apple_and_Google_will_kill_the_password_?taxonomyId=15&pageNumber=2.

200. *See, e.g.*, Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1653 (2011).

201. Michelle Madejski et al., The Failure of Online Social Network Privacy Settings (2011) (Columbia Univ. Computer Science, unpublished Technical Report No. CUCS-010-11), *available at* http://academiccommons.columbia.edu/catalog/ac:135406.

environment.[202] In time, adaptive privacy, and the audiences these adapted zones encompass, will become increasingly important.

C. Identification

Identification is both one of the central aspects of online obscurity and a major component of general information privacy law.[203] Simply put, information that cannot be linked to a person poses a reduced threat to that person's privacy. While anonymity is central to many privacy disputes,[204] pseudonymity often gets short shrift in legal debates. Yet the use of identification variants (ID variants) and pseudonyms is a key component of online obscurity. Like passwords, ID variants and pseudonyms can serve two functions: (1) they can protect the discloser or subject of information by unlinking content from identity, and (2) if ID variants or pseudonyms are readily apparent, they can signal to the consumer of information that the disclosure is sensitive or private, invoking the concept of confidentiality as well as obscurity.

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.[205] For example, an individual that maintains a pseudonymous 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 to the selective crafting of the online persona. In the context of the online obscurity framework, identification is defined as the existence of an irrefutable piece of information that links content online to the individual's person.

If the identity of the discloser or subject of the content is clear, the information is more obvious and therefore less obscure. Information associated with an ID variant or pseudonym that is not easily traceable to a real identity,

---

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

203. *See, e.g.*, Ohm, *supra* note 114.

204. *Id.*

205. J. Donath & d. boyd, *Public Displays of Connection,* 22 BT TECH. J. 71 (2004) 73–77; danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship,* 13 J. COMPUTER-MEDIATED COMM. 210, 213 (2007), *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html ("The public display of connections is a crucial component of SNSs. The Friends list contains links to each Friend's profile, enabling viewers to traverse the network graph by clicking through the Friends lists.").

on the other hand, is much more obscure, making it more likely to receive the benefit of privacy protections.

D. Clarity

Although online information is often easily discoverable, important aspects of that information may be incomprehensible. Information might be intentionally vague or incomplete. Sometimes information in one domain is separated by medium, tool, or linkage from another piece in order to make it more obscure and thus more protected.[206] Lack of clarity, meant here as the ability to be easily understood, 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. In her ethnographic analysis, danah boyd noted that her teenage respondents 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."[207] According to boyd, this process is known as "steganography," "an ancient technique where people hide messages in plain sight."[208]

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, which is facilitated by shared interpersonal knowledge and linguistic styles. When conversing, shared knowledge within groups allows individuals to "presuppose."[209] 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 conversation overheard, but she will likely lack the information necessary for true comprehension or identification of the conversational subjects. This lack of clarity renders the overheard conversation obscure. The same is true for online communication, much of which is clouded by in-group communication that frustrates clarity.[210]

---

206. *See, e.g.*, Stutzman & Hartzog, *supra* note 7.

207. 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.

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

209. *See* Goffman, *supra* note 23, at 1. Goffman states that "A *presupposition* (or assumption, or implication, or background expectation) can be defined very broadly as a state of affairs we take for granted in pursuing a course of action. We can perform these acts of faith without 'doing' anything." *Id.*

210. *See, e.g.*, Martin Tanis & Tom Postmes, *Social Cues and Impression Formation in CMC*, 53 J. COMM. 676 (2003); Joseph B. Walther, *Selective Self-Presentation in Computer-Mediated*

A finding that information is unclear to the extent that it is unlikely to be understood by unintended recipients renders it more obscure, making it more likely to receive the benefit of privacy protections.

In sum, our conceptualization of online obscurity is simultaneously broad enough to remain adaptable to new technologies while sufficiently defined 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 demonstrated that obscurity is a central concept to online privacy that has been glossed over by courts. We hypothesized that online disputes have not utilized obscurity because the concept has not been well defined or conceptualized. Now that we have offered a useful framework, we will consider how obscurity could ameliorate tension between privacy law and user expectations regarding online information. Generally, online obscurity can frame the online privacy analysis and become a remedy or obligation. More 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.

We emphasize up front that remedies based on 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 doctrines, such as confidentiality or anonymity.

However, this does not mean obscurity is a useless concept. Obscurity can be a meaningful legal protection precisely *because* it is not as protective as concepts like confidentiality or anonymity.[211] Obscurity could protect information that is less sensitive or sensitive in fewer contexts if it is ineligible for more robust privacy protections. For example, many privacy protections, such as the disclosure tort, do not apply to information known by a significant number of third parties.[212] However, the focus of online obscurity is 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 secret.[213] They might not want to keep this information from being

Communication: Hyperpersonal Dimensions of Technology, Language, and Cognition, 23 COMPUTERS HUM. BEHAV. 2538 (2007).

211. In their most extreme forms, confidentiality demands a complete restriction on the dissemination of information and anonymity demands a complete inability to identify a target. *See* Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 675 (2012); Gary T. Marx, *What's in a Name? Some Reflections on the Sociology of Anonymity*, 15 INFO. SOC'Y 99 (1999).

212. *See, e.g.*, Strahilevitz, *Reunifying Privacy Law*, *supra* note 188.

213. *See, e.g.*, Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

discovered or understood by everyone; they might just want to keep it away from certain people. This is where obscurity becomes useful. Obscurity obligations would not aim to completely curtail information disclosure; rather, they would seek to minimize the likelihood of discovery, comprehension, or contextualization.

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 Part 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."[214] Yet, notably, courts often give legal significance to code-based solutions, such as passwords and encryption, that 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 online disclosures are public. This is largely an arbitrary distinction in light of how users actually perceive and expect privacy, as described in Part II. But adopting the distinction is tempting because of its manageability—courts can easily identify when Internet users employ passwords. This is particularly true compared to the relative difficulty of trying to understand someone's "reasonable expectation of privacy" in any given context.[215] Hence, any conceptualization of online obscurity must be concrete, easy to understand, manageable, and as objective as possible.

---

214. *See, e.g.*, Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010). The court found no reasonable expectation of privacy in social network sites, 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. Fleming & Joseph M. Herlihy, *What Happens When the College Rumor Mill Goes Online? Privacy, Defamation and Online Social Networking Sites*, 53 BOS. B.J. 16 (2009)).

215. *See, e.g.*, Solove, *supra* note 133, at 1511–12 ("The 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.'").

Despite numerous cases on the issue, courts lack a generally accepted framework or test for determining when online information is public.[216] For example, in *Moreno v. Hanford Sentinel*, 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.[217] The court denied that the poem was private because it had already been made public by the plaintiff.[218] The court found that the plaintiff had "publicized her opinions about [her hometown] by posting the Ode on MySpace.com, a hugely popular Internet site."[219] The court held that the plaintiff's failure to use protective measures such as privacy settings or password protection was significant in determining whether she could reasonably expect online information to be private.[220]

By equating "theoretically accessible" with "public," the *Moreno* court overlooked the many ways individuals obfuscate information online. Under the court's reasoning, the plaintiff might have had a reasonable expectation of privacy if she protected the website with a password.[221] The court failed to consider the other factors of obscurity: whether the poem was visible to search engines, whether the plaintiff used her real name or an ID variant, and whether the poem was easily understood as a representation of the plaintiff's hometown. Instead, theoretical accessibility of the poem was the *sine qua non* for rendering the information public, thus denying it protection under privacy laws.

A useful conception of online obscurity would be helpful in cases like *Moreno*. Instead of an arbitrary distinction based on password use, courts should determine where information falls 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 all of these elucidating factors would be deemed completely obscure and most deserving of privacy protections. Of course, in the middle lies the gray area, where the information has at least one, but not all, of the indicia of online obscurity.

To that end, courts should 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?

---

216. Strahilevitz, *supra* note 85, at 920–21.

217. 91 Cal. Rptr. 3d 858 (Ct. App. 2009).

218. *Id.*

219. *Id.* at 862.

220. *Id.* ("Cynthia's affirmative act made her article available to any person with a computer and thus opened it to the public eye.").

221. *Id.*

3. Was the information associated with an ID variant or pseudonym that is not easily traceable to a real identity?
4. Was the information likely to be understood by unintended recipients?

By analyzing these factors independently and as a whole, courts will arrive at a more nuanced decision regarding whether to afford information privacy protections.

B. Obscurity as a Protective Remedy

In addition to playing a key role in the privacy analysis, a well-conceptualized obscurity framework would serve as a protective remedy. Specifically, obscurity would either be conferred as a benefit or provided as a 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 less effective, but also less costly, remedy than complete confidentiality, anonymity, or the "right to be forgotten."[222] 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 by mandating the redaction of personal identifiers such as social security numbers from some public records.[223] Several proposed privacy protection laws focus on the collection of "personally identifiable information."[224] Courts and lawmakers should expand the scope of these protection laws. Pseudonymous litigation has been proposed by some as a way

222. *See, e.g.*, Adam Thierer, *Erasing Our Past on the Internet,* FORBES (Apr. 17, 2011, 1:46 PM), http://www.forbes.com/sites/adamthierer/2011/04/17/erasing-our-past-on-the-internet/; MAYER-SCHÖNBERGER, *supra* note 13; Ciaran Giles, *Internet 'Right to Be Forgotten' Debate Hits Spain*, BOSTON.COM (Apr. 20, 2011), http://www.boston.com/news/world/europe/articles/2011/04/20/internet_right_to_be_forgotten_debate_hits_spain/.

223. The E-Government Act of 2002 instructed that personal identifiers, such as Social Security numbers and names of minor children, be redacted from federal court filings. Pub. L. No. 107-347, 116 Stat. 2899 (2002). *See also* Peter W. Martin, *Online Access to Court Records—From Documents to Data, Particulars to Patterns,* 53 VILL. L. REV. 855, 868 (2008) ("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.").

224. *See, e.g.*, Venkat Balasubramani, *A Look at the Commercial Privacy Bill of Rights Act of 2011*, ERIC GOLDMAN: TECH. & MKTG. BLOG (Apr. 20, 2011, 9:03 AM), http://blog.ericgoldman.org/archives/2011/04/a_look_at_the_c.htm. *See also* Tanya Forsheit, *Breaking Down the Boucher Bill*, INFORMATIONLAWGROUP (May 12, 2010), http://www.infolawgroup.com/2010/05/articles/behavioral-advertising/breaking-down-the-boucher-bill/.

to ease the publicity inherent in filing a lawsuit.[225] But this protection focuses on only one aspect of obscurity—identification. As we have described, there are other ways to protect information with online obscurity.

Online obscurity is a useful middle-ground protection. By embracing obscurity, courts and lawmakers can avoid the complete opacity created by traditional privacy protections, such as sealed records. At the same time, courts and lawmakers should provide obscurity in situations where they are not willing to provide total secrecy or confidentiality. Hence, obscurity could protect certain privacy interests while also promoting the dissemination of information. The FTC and other governmental agencies should consider obfuscation as a valid technique for protecting certain kinds of consumer information.[226]

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 would curtail certain abuses of "big data"[227] and effectuate the spirit of the OECD Privacy Guidelines.[228] Thus, obscurity represents a compromise between those seeking to publish or access information and those seeking to restrict it. The proper distinction, which is beyond the scope of this Article, is between which information requires confidentiality or secrecy and which information is adequately protected by online obscurity.

As Part II of this Article demonstrated, Internet users desire and rely upon the obscurity of some of their online information. Like any other desirable result, obscurity could be a benefit for which parties negotiate in both legal disputes and commercial transactions. For instance, if an individual sues a website for public disclosure of private facts, the parties might voluntarily agree on the website blocking the information from being searched instead of completely deleting it or awarding the plaintiff a monetary settlement.[229] This

225. *What Does It Mean to File a Suit Pseudonymously?*, WITHOUT MY CONSENT, http://www.withoutmyconsent.org/quick_link/what-does-it-mean-file-suit-pseudonymously (last visited Nov. 10, 2012). *See* Strahilevitz, *Pseudonymous Litigation*, *supra* note 188.

226. Commercial data brokers also collect obscure but available information online and should be regulated under this approach. *See, e.g.*, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect 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.

227. JANNA QUITNEY ANDERSON & LEE RAINIE, PEW INTERNET & AM. LIFE PROJECT, BIG DATA: EXPERTS SAY NEW FORMS OF INFORMATION WILL HELP PEOPLE BE MORE NIMBLE AND ADAPTIVE, BUT WORRY OVER HUMANS' CAPACITY TO UNDERSTAND AND USE THESE NEW TOOLS WELL (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_Future_of_Internet_2012_Big_Data.pdf.

228. *OECD Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data*, OECD, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Nov. 10, 2012) (setting forth data privacy guidelines for industry and governments that enable the transborder transfer of information).

229. Plaintiffs in privacy disputes have an increasingly difficult time collecting monetary damages. *See, e.g.*, Daniel J. Solove, *The Slow Demise of Defamation and the Privacy Torts*,

compromise lowers the likelihood that other parties, such as employers, find the information while allowing the website to keep the information posted.

Again, online obscurity as a protective measure is hardly suitable for information likely to be shared and widely linked to throughout the Internet. Some information, particularly concerning celebrities and public officials, must be kept secret or highly confidential to avoid wide distribution on the Web. Additionally, it is very difficult to predict what information will go viral online. Information can be irrelevant to most people while potentially harmful to some—for example, photos of a high school student with alcohol may be viewed by admissions counselors. Most people have no interest in viewing or incentive to look for these pictures, so obscurity would benefit those users who might be harmed by such information.

A similar argument is made for the average job applicant. Many professionals assert that your "online resume"—what employers can quickly find about you online—is just as, if not more, important than your actual resume.[230] However, only obvious, nonobscure information is likely to be found or read by employers. According to Michael Fertik and David Thompson, only information that can be found by an average user in five minutes or less is part of your online resume.[231] Thus, if a job applicant is concerned about how an embarrassing or personal photo might affect her job prospects, it is possible—by burying the photo in obscurity—to minimize the likelihood a potential employer would find it in a routine background search.

Obscurity's usefulness as a benefit or protection is illustrated by the fact that a number of groups have already entered the obscurity business. Reputation.com, for example, is a company that helps customers protect their reputations through various techniques, including suppressing search results to make harmful information more obscure.[232]

A full exploration of online obscurity as a protective remedy is beyond the scope of this Article. However, this Section shows how online obscurity might serve as a legal benefit or halfway point between two extremes of no protection and total secrecy.

HUFFINGTON POST (Oct. 11, 2010, 4:52 PM), http://www.huffingtonpost.com/daniel-j-solove/the-slow-demise-of-defama_b_758570.html.

230. *See, e.g.*, MICHAEL FERTIK & DAVID THOMPSON, WILD WEST 2.0: HOW TO PROTECT AND RESTORE YOUR ONLINE REPUTATION ON THE UNTAMED SOCIAL FRONTIER 26 (2010) ("[F]or 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 résumé.").

231. *Id.* at 26.

232. *See* REPUTATION.COM, http://www.reputation.com/reputationdefender (last visited Nov. 10, 2012). One physician 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." Taylor Doherty, *Potti Hires Online Reputation Manager*, CHRONICLE (Apr. 14, 2011) http://dukechronicle.com/article/potti-hires-online-reputation-manager.

C. Share Alike: An Agreement to Maintain Obscurity

The current discussion surrounding online agreements and privacy centers on confidentiality agreements and consent to obtain and use personal information.[233] Explicit confidentiality agreements can be awkward to obtain in the course of social interaction.[234] By agreeing to keep information confidential, users are largely prohibited from disclosing the information at all.

Online obscurity is an alternative to the standard confidentiality agreement. Instead of binding adherents to a duty of confidentiality, disclosers of information could impose a duty on potential recipients of information to maintain the obscurity of that information. For example, social network site users could promise to keep information invisible from search engines, to protect further disclosures of information with privacy settings, or to ensure disclosers' names remain unassociated with the disclosed information.

This approach highlights online obscurity's reliance on Nissenbaum's theory. Website user agreements would 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 beforehand specific factors critical to online obscurity, adherents would have a clearer picture of the practices that would breach their agreement.

Agreements to maintain online obscurity could resemble the "share alike" principle embedded in Creative Commons and open software licenses. Creative Commons is an organization that offers a variety of copyright licenses that allow creators to choose how their work can be utilized and the terms on which it can be shared.[235] Under a "share alike" provision, a copyright owner licenses a user to do things like remix, tweak, and build upon the work in a noncommercial way, as long as the user licenses his or her new creation under the identical terms stipulated by the original copyright owner.[236] 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 is introduced in established contexts. Consider facial-recognition

---

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

234. *See, e.g.*, Sandra Braman & Stephanie Roberts, *Advantage ISP: Terms of Service as Media Law*, 5 NEW MEDIA & SOC'Y 422 (2003); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 460 (2006); 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 1 (Mar. 29, 2010) (Ass'n for the Advancement of Artificial Intelligence Press, unpublished Technical Report No. SS-10-05), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1580111.

235. *About the Licenses*, CREATIVE COMMONS, http://creativecommons.org/licenses/ (last visited Nov. 10, 2012).

236. *Id.*

technology and social media: social network sites or sharing sites like Facebook often promise to respect both the user's privacy and her or his privacy settings.[237] An important function of some of these websites is the ability to tag photos.[238] 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 would constitute a breach of that promise.

Agreements between Internet users could also incorporate online obscurity by including 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. This advances Lior Strahilivetz's social networks theory of privacy.[239] Obscurity could be an effective way to implement that theory by lowering the risk of others accessing or understanding information, which could bolster the reasonableness of an expectation of privacy. Social networks are difficult to define, but it is easier for users to respect specific obfuscation techniques, such as refraining from reposting information on web pages indexed by search engines, than attempt to guess the limits of these "blurry-edged networks."[240]

As with the previous potential applications of online obscurity, a full explication of a duty to maintain obscurity is beyond the scope of this Article and will be addressed in future research. However, this Section illuminates how agreements regarding personal information can encompass more than just duties of confidentiality. A duty to maintain obscurity is a desirable and manageable provision for parties entering into personal information agreements 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 of significant public exposure.[241] 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

237. *See* Hartzog, *supra* note 200, at 1636–38.

238. *See, e.g.*, *Posting*, TUMBLR, http://www.tumblr.com/docs/en/posting (last visited Nov. 10, 2012); *Tagging Photos*, PICASA, http://support.google.com/picasa/answer/106209/?& (last visited Nov. 10, 2012); *What Is Tagging and How Does It Work?*, FACEBOOK, https://www.facebook.com/help/?faq=13407 (last visited Nov. 10, 2012) (discussing how to tag posts).

239. Strahilevitz, *supra* note 85, at 920–21.

240. *See* Gelman, *supra* note 1, at 1317–19.

241. ALDOUS HUXLEY, THOSE BARREN LEAVES 19 (1925).

obscurity. Genuineness only thrives in the dark. Like celery."[242] 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. 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 Article, we have made the case for obscurity online. While obscurity is an everyday phenomenon, we bring our practices of obscurity online as well. As our online and off-line networks interact, and online environments move away from anonymity 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 heterogeneous, nonymous environments.

We have argued that the law has failed to embrace online obscurity 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: (1) search 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. Information that is entirely unobscure is completely obvious, and vice versa. Courts should engage in a case-by-case analysis of the factors to determine the degree of online obscurity.

This Article also proposed ways to implement obscurity as a remedy to ease the tension between privacy law and the expectations of Internet users. This framework could be applied in online privacy disputes as an analytical tool or as part of an obligation. Obscurity could serve 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 implementation of online obscurity are meant to be an introduction, not the final word. Additional research and

242. *Id.*

analysis are required to fully explore how the law might utilize online obscurity. 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 off-line 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.