2013

Obscurity by Design

Woodrow Hartzog
Boston University School of Law

Frederic D. Stutzman

OBSCURITY BY DESIGN

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

Abstract: Design-based solutions to confront technological privacy threats are becoming popular with regulators. However, these promising solutions have left the full potential of design untapped. With respect to online communication technologies, design-based solutions for privacy remain incomplete because they have yet to successfully address the trickiest aspect of the Internet—social interaction. This Article posits that privacy-protection strategies such as "Privacy by Design" face unique challenges with regard to social software and social technology due to their interactional nature.

This Article proposes that design-based solutions for social technologies benefit from increased attention to user interaction, with a focus on the principles of "obscurity" rather than the expansive and vague concept of "privacy." The main thesis of this Article is that obscurity is the optimal protection for most online social interactions and, as such, is a natural locus for design-based privacy solutions for social technologies. To that end, this Article develops a model of "obscurity by design" as a means to address the privacy problems inherent in social technologies and the Internet.

---

[*] Assistant Professor of Law, Samford University's Cumberland School of Law; 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, Travis Breaux, Ryan Calo, Will DeVries, Chris Hoofnagle, Jen King, Helen Nissenbaum, Elizabeth Porter, Sasha Romanosky, Zahr Said, Jeremy Sheff, Daniel Solove, Kathy Strandburg, the faculty at H. John Heinz III College at Carnegie Mellon University, Samford University's Cumberland School of Law and the participants of workshops and presentations hosted by the Privacy Law Scholars Conference, Google, Elon University School of Law, CSCW 2012 Reconciling Privacy with Social Media Workshop, and the Washington Law Review. 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).

INTRODUCTION

Privacy by design, that is, "the philosophy and approach of embedding privacy into the design specifications of various technologies," promises to alter the law's largely reactive approach to privacy threats.[1] Government and industry are gradually embracing privacy by design and other design-based strategies to protect Internet users.[2] To ensure wide applicability, the Privacy by Design approach offers little domain-specific guidance. However, with the growth of the Internet and social technologies, designing usable and effective privacy for technologically mediated social interaction (such as the interaction afforded by social media) is an urgent challenge, one deserving of investigation.

---

1. ANN CAVOUKIAN, PRIVACY BY DESIGN 1 (2009), *available at* http://www.ipc.on.ca/images/Resources/privacybydesign.pdf [hereinafter CAVOUKIAN, PRIVACY BY DESIGN]; *see* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE SEVEN FOUNDATIONAL PRINCIPLES (2009), *available at* http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf [hereinafter CAVOUKIAN, SEVEN FOUNDATIONAL PRINCIPLES].

2. *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC); *Report of the Art. 29 Data Protection Working Party and Working Party on Police and Justice on The Future of Privacy* at 3, (Dec. 1, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf; FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC, PROTECTING CONSUMER PRIVACY].

Over the past forty years, regulators and technologists have expended significant effort managing the privacy risk inherent in the collection and storage of personal information.[3] In the era of social media and behavioral tracking, the vast databases (i.e., "big data") that store personal information pose significant threats, but these databases and their parent organizations are far from the only threat to privacy on the Internet. The growth of the social web has demonstrated that information sharing inherent in the management of online relationships through social media present their own privacy challenges. As billions of individuals participate in social media, the vast amount of information disclosed and transferred between individuals—an inherent requirement for social interaction online—poses a new class of privacy threat that should be addressed through design.[4]

Addressing the vexing privacy problems of the social web is a challenging task. Few can agree on a conceptualization of privacy,[5] much less how to protect privacy in our social interactions by design.[6] There are a number of practical reasons why privacy by design has avoided the social side of the user interface. The translation of regulation to implementation is a complex process and may be more efficient when applied to formal technologies (e.g., databases, protocols).[7] Additionally, there is little guidance regarding how designers should approach the implementation of privacy by design in a contextually variant, interactional space. Many substantive protections entailed in privacy by design are effectuated on the "back end" of technologies, such as data

---

3. ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY, Version 1.91 (2012), *available at* bobgellman.com/rg-docs/rg-FIPShistory.pdf.

4. *See, e.g.*, DANIEL J. SOLOVE, THE FUTURE OF REPUTATION (2007); danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 133 (David Buckingham ed., 2008); Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315 (2009); James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009); Fred Stutzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, J. PRIVACY & CONFIDENTIALITY, 2012, at 7, *available at* http://repository.cmu.edu/jpc/vol4/iss2/2/.

5. *See, e.g.*, SOLOVE, *supra* note 4; ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Stephen T. Margulis, *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, 59 J. SOC. ISSUES 411 (2003).

6. *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH L.J. 1409, 1421 (2011) ("Privacy by design is an amorphous concept."); Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, (New York Univ. Sch. of Law, Working Paper No. 12-43, 2012), *available at* https://www.privacyassociation.org/media/pdf/events_and_programs/Privacy%20by%20Design-A%20Counterfactual%20Analysis.pdf.

7. Seda Gürses, Carmela Troncoso & Claudia Diaz, Address at the Computers, Privacy & Data Prot. Annual Conference: Engineering Privacy by Design (Jan. 29-30, 2011).

security through encryption, data minimization techniques, anonymity, and structural protection though organizational prioritization of privacy.[8] However, the design of social technologies must consider "front end" privacy concerns such as privacy settings, search visibility, password protections, and the ability to use pseudonyms.[9]

The answer to these challenges might lie in refining the goal for the design of social technologies. The current goal of design solutions is "privacy," which is too broad and opaque to provide meaningful guidance in designing social technologies. Indeed, one conceptualization of privacy, secrecy, can be seen as antithetical to the notion of social interaction. This Article recommends looking to the related concept of obscurity. Empirical evidence demonstrates that Internet users aim to produce and rely upon obscurity to protect their social interaction online.[10] The concept of online "obscurity," defined here as a context in which information is relatively difficult to find or understand, is a much more defined and attainable goal for social technology designers. Obscurity is more flexible than some conceptualizations of privacy and also more feasible to implement. Moreover, obscurity involves more than prohibitions on conduct; internet users can actively produce obscurity themselves.

The main thesis of this Article is that obscurity is an optimal protection for social interaction online and, as such, is a useful concept and design pattern when addressing front-end (i.e., user-facing) privacy concerns. Therefore, the purpose of this Article is to introduce and develop the concept of "obscurity by design" as a model for design-based privacy solutions in social technologies. In doing so, we provide organizations who wish to embrace privacy-protective design principles with a useful set of tools for approaching these interactional privacy concerns.

Part I of this Article reviews the broader concept of privacy by design, including its strengths, the challenges to its implementation, and its missed opportunity in failing to account for the front-end design of social technologies. Part II sets forth our conceptualization of obscurity, including the four major factors of online obscurity: (1) search visibility,

---

8. *See* GELLMAN, *supra* note 3.

9. *See* Frederic Stutzman & Woodrow Hartzog, *Boundary Regulation in Social Media*, *in* PROCEEDINGS OF THE ACM 2012 CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK 769 (2012), *available at* http://dl.acm.org/citation.cfm?id= 2145320&bnc=1 [hereinafter Stutzman & Hartzog, *Boundary Regulation*]; Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013) [hereinafter Hartzog & Stutzman, *Online Obscurity*].

10. *See* Hartzog & Stutzman, *Online Obscurity*, *supra* note 9.

(2) unprotected access, (3) identification, and (4) clarity. This Article proposes that the four factors of online obscurity constitute a set of principles that designers should consider when building privacy into social technologies. Finally, Part III proposes a model to implement obscurity by design. This model suggests that obscurity by design can be effectuated through a combination of technologies, policies, and behavioral interventions.

I. PRIVACY BY DESIGN MUST BE CLARIFIED TO APPLY TO THE USER INTERFACE OF SOCIAL MEDIA

In recent years, consumer technologies have embraced the broad collection and storage of personal information. Behavioral advertising, consumer forecasting, and geolocational systems have pushed—and created new—boundaries for the collection of data about users.[11] While many industries argue that increased data will lead to better products and predictions,[12] the collection and storage of this data potentially opens consumers and companies to novel risk.

Early approaches to protect the information and privacy rights of consumers were to punish violators by utilizing torts, statutes, and regulations to levy fines and injunctions.[13] These "reactive" approaches remain in use, but the challenges of web-scale technologies, and the scale of risks such as breach or hacking, require a proactive approach to privacy protection.[14] These modern "design-based" solutions to privacy

---

11. *See, e.g.*, FTC, PROTECTING CONSUMER PRIVACY, *supra* note 2; FTC, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 3 (2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf [hereinafter FTC, MOBILE PRIVACY DISCLOSURES] ("[M]obile devices can reveal precise information about a user's location that could be used to build detailed profiles of consumer movements over time and in ways not anticipated by consumers. Indeed, companies can use a mobile device to collect data over time and 'reveal[] the habits and patterns that mark the distinction between a day in the life and a way of life.'") (quoting United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010)); Josh Halliday, *Facebook Users Unwittingly Revealing Intimate Secrets, Study Finds*, GUARDIAN (Mar. 11, 2013), http://www.guardian.co.uk/technology/2013/mar/11/facebook-users-reveal-intimate-secrets; Press Release, FTC, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://www.ftc.gov/opa/2012/12/databrokers.shtm.

12. *See, e.g.*, JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY (2011), *available at* http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

13. *See, e.g.*, Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY (2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271; Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008).

14. *See, e.g.*, FTC, PROTECTING CONSUMER PRIVACY, *supra* note 2; Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

focus on concepts such as data minimization, security, information policy, and disclosure of information practices. This proactive approach to privacy has crystallized in the privacy-by-design movement, which seeks to build "the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems."[15] This Part will review the history of privacy by design and review the challenges to its implementation in various contexts, notably the user interface of social media.

A. Privacy by Design Challenges Organizations to Rethink Established Approaches to Privacy

Privacy by design can best be thought of as a technological design framework; when this framework is embraced in the design phase, the resultant technology should embody privacy protection. In this sense, "privacy" is not an afterthought or a security treatment, but an essential value in the design and construction process.

The privacy by design movement can be traced back to Dr. Ann Cavoukian, the Information & Privacy Commissioner of Ontario, Canada.[16] Cavoukian's approach to privacy by design is illustrated in numerous white papers,[17] as well as an edited volume of the journal *Identity in the Information Society*.[18] Cavoukian's approach to privacy by design argues for the inclusion of Fair Information Principles into the design of technologies. These principles include:

1. Recognition that privacy interests and concerns must be addressed proactively;
2. Application of core principles expressing universal spheres of privacy protection;
3. Early mitigation of privacy concerns when developing information technologies and systems, throughout the entire information life cycle—end to end;
4. Need for qualified privacy leadership and/or professional input;
5. Adoption and integration of privacy-enhancing *technologies*

15. CAVOUKIAN, PRIVACY BY DESIGN, *supra* note 1, at 1.; *see* CAVOUKIAN, SEVEN FOUNDATIONAL PRINCIPLES, *supra* note 1; Rubinstein, *supra* note 6, at 1421–22; Rubinstein & Good, *supra* note 6, at 1, 5–7.

16. CAVOUKIAN, PRIVACY BY DESIGN, *supra* note 1, at 1; CAVOUKIAN, SEVEN FOUNDATIONAL PRINCIPLES, *supra* note 1.

17. Rubinstein & Good, *supra* note 6, at 6.

18. *See generally Privacy by Design: The Next Generation in the Evolution of Privacy*, 3 IDENTITY INFO. SOC'Y 247 (2010) (special issue devoted to privacy by design), *available at* http://link.springer.com/journal/12394/3/2/page/1.

(PETs);

6. Embedding privacy in a positive-sum (not zero-sum) manner so as to enhance both privacy and system functionality; and
7. Respect for users' privacy.[19]

The privacy by design approach has proven to be a useful innovation within the design community, where emphasis is often placed on PETs or *ex post* remedies. Using a process lens, privacy by design argues that privacy is a critical part of the socio-technical infrastructure of technologies, and that privacy is both a value and a tangible component that must be included in technologies. To accomplish this goal, Cavoukian argues that privacy by design should be valued through the organizational hierarchy (e.g., qualified leadership) and that the privacy outcomes should be positive for the user.[20] In a sense, privacy by design provides both process and infrastructure for the inclusion of privacy as both a value and a tangible good in the design of technical systems (as well as organizational practices and physical design, notes Cavoukian).[21]

In reaction to failures of privacy enhancing technologies or *ex post* measures as a robust privacy strategy, privacy organizations, government regulators, and industry groups are moving toward privacy by design as a potential information-age remedy to privacy threats. In 2012, the Federal Trade Commission (FTC) privacy framework, "Protecting Consumer Privacy in an Age of Rapid Change," strongly encouraged companies to adopt privacy-by-design approaches to their business and technical operations.[22] Furthermore, the European Data Protection Supervisor also strongly recommended privacy by design as a requirement in the forthcoming data protection regulation—potentially requiring firms in the EU, as well as those doing business with EU firms, to follow privacy by design under threat of fines or other legal action.[23] The adoption of privacy by design by regulatory agencies as a guideline or requirement would require organizations to change the way privacy is treated in the process of technology design. Such a regulatory move

---

19. CAVOUKIAN, PRIVACY BY DESIGN, *supra* note 1, at 1; *see* CAVOUKIAN, SEVEN FOUNDATIONAL PRINCIPLES, *supra* note 1.

20. *See* CAVOUKIAN, PRIVACY BY DESIGN, *supra* note 1, at 3.

21. *See id.* at 4–5.

22. *See* FTC, PROTECTING CONSUMER PRIVACY, *supra* note 2. Privacy by design was also one of the "three core principles" called upon by the FTC in a recent report on mobile app privacy. FTC, MOBILE PRIVACY DISCLOSURES, *supra* note 11, at 6.

23. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Comprehensive Approach On Personal Data Protection in the European Union*, COM (2010) 609 final (Nov. 4, 2010).

would be noteworthy, as there are a number of challenges to its implementation.

B. Obscurity Can Improve Privacy by Design

The adoption of privacy by design as a universal approach to privacy poses a set of significant challenges for implementers. General criticisms include a lack of incentives for the deployment of privacy by design, questions about its enforceability, the inherent organizational challenges of adopting and applying new privacy practices, and the technical hurdles of a privacy by design development model.[24] While these criticisms are sharp, it is clear that privacy by design is a useful way of addressing the privacy challenges that technology designers face. The design of technology is an interdisciplinary problem that involves the coordination of engineers, managers, lawyers, policymakers, and executives within an organization. The privacy by design approach helps address these challenges by setting forth values that disparate parts of the organization can embody in the design process. Of course, this is often easier said than done.

As outlined by Ira Rubinstein, two of the primary challenges facing privacy by design include a weak specification of the privacy by design approach and lack of incentives for the firm to adopt it.[25] Here we concentrate on Rubinstein's question of incentives. Rubinstein considers why firms would adopt privacy by design (as well as PETs), exploring endogenous motivation, market demand, and regulatory potential.[26] To the question of endogenous motivation, firms are differentially motivated towards privacy based on data collected, tolerance of risk, and economic impact of privacy breaches. Therefore, motivation as an endogenous trait is not uniformly distributed across firms.[27] Rubinstein then questions consumer valuation of privacy and PETs, arguing that there is little market demand for privacy goods (even non-zero-sum goods).[28] Finally, Rubinstein explores the potential for regulatory enforcement, finding that regulatory capability to enforce privacy by design to be premature due to challenges in establishing consent orders based on privacy by design language.[29]

---

24. *See generally* Rubinstein, *supra* note 6.
25. *See id.* at 1414–44.
26. *See id.* at 1414–53.
27. *See id.* at 1436–40.
28. *See id.* at 1433–36.
29. *See id.* at 1444–53.

As Cavoukian notes, the premise of privacy by design is to construct technologies that embody the principles of Fair Information Practices.[30] The roadmap to the creation of these technologies is not one that can be directly specified in the sense that there is a linear set of steps to follow. This is the specification problem described by Rubinstein.[31] The design of a product (specifically, software) requires the translation of requirements (e.g., semantic descriptions of functionality) into code that can be compiled and executed. In the context of a software product team, such a translation can be facilitated when requirements are precise and product managers know designers' limits and capabilities. However, even in the context of highly skilled teams, the requirements engineering phase of product design is non-trivial. With regulatory oversight of a process or design, new requirements engineering challenges emerge.[32] Regulatory requirements are often vague, describing a generic process that can apply to many different types of systems; ensuring compliance with such a process is often highly challenging.[33] As the privacy by design specifications are inherently generic, translation of these requirements into design is a significant challenge.

Finally, we call on Rubinstein's taxonomy of front-end and back-end technologies when describing the components of a system.[34] Rubinstein's point is clear and important—systems are multi-faceted and the user experience has many different components.[35] Systems are commonly not built as a cohesive whole, but as parts that are placed together to accomplish a goal. It is important to think about how a privacy risk model varies for different components of the system. For example, a website might have a front end (the website itself) and a back end (the data store). The risk model for these two components is different in that privacy attacks or problems can vary substantially. A formal system, such as a database, has a known universe of threats that can be guarded systematically. A front end, on the other hand, may invoke a range of threats, from the social to the technical. The heterogeneity of these threats makes it harder to apply formal privacy logics, leading to a potentially greater propensity to design privacy for

30. *See* CAVOUKIAN, PRIVACY BY DESIGN, *supra* note 1, at 1.

31. *See* Rubinstein, *supra* note 6, at 1423–31.

32. *See* Travis D. Breaux & Annie I. Antón, *Analyzing Regulatory Rules for Privacy and Security Requirements*, 34 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 5, 5, 17–19 (2008).

33. *See id.* at 5.

34. *See* Rubinstein, *supra* note 6, at 1421–31.

35. *See id.*

formal systems only.[36]

Thus, there are many roadblocks to a large-scale adoption of privacy by design, such as challenges to the demand for, feasibility of, and technical capacity to implement this approach. This is further complicated by the nature of privacy, where risks are both endogenous (that is, the product of a known set of risks inherent to the technology) and exogenous (the product of external, often unknowable risks) to the technology.[37] We see an illustration of this with social media, where individuals interact with systems (where endogenous risk can be known), as well as with other individuals (where exogenous risks emerge) within the system. This raises privacy challenges that have not been seen before in other interactive technologies. For this reason, we use social media as the case we examine in the remainder of this Article.

Externally, conceptualizing privacy within the context of social technologies in a way that is workable for design-based solutions has proven elusive.[38] As previously mentioned, there is no general agreement on what the term "privacy" means in a social context, much less how Internet design can protect it.[39] While many scholars and regulators have agreed that "back end" protections, such as those provided for in the fair information practices,[40] are critical design-based protections, these background safeguards fail to address the "front end" of the Internet, which involves user interfaces designed to facilitate online social interaction.

Social interaction is messy, unpredictable, and contextual with a vengeance. Consequently, any design rules or guidelines seem destined either to be inconsistently effective or miss the mark entirely. But the social web is now too large to exclude from the realm of design-based solutions. Social network sites like Facebook have over one billion users.[41] Even commercial and news websites are incorporating social aspects into their user experience.[42] Thus, the time has come for design

---

36. *See* Gürses, Troncoso & Diaz, *supra* note 7; Sarah Spiekermann & Lorrie Faith Cranor, *Engineering Privacy*, 35 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 67 (2011).

37. *See* Paul Dourish & Ken Anderson, *Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena*, 21 HUM.-COMPUTER INTERACTION 319 (2006).

38. *See, e.g.*, Gelman, *supra* note 4; Hartzog & Stutzman, *Online Obscurity*, *supra* note 9.

39. *See* Hartzog & Stutzman, *Online Obscurity*, *supra* note 9.

40. The FTC has identified the major substantive principles of privacy by design as data security, reasonable collection limits, sound retention practices, and data accuracy. FTC, PROTECTING CONSUMER PRIVACY, *supra* note 2, at 22–32.

41. *See Key Facts*, FACEBOOK, http://newsroom.fb.com/Key-Facts (last visited Apr. 17, 2013).

42. *See Community Forum*, AMAZON.COM, http://www.amazon.com/forum/community?_encoding=UTF8&cdOpenPostBox=1 (last visited Apr. 17, 2013); *Community*

guidelines to protect privacy in this social medium.

II. BETTER LIVING THROUGH OBSCURITY

Most conceptualizations of privacy on the Internet seem to break down at the social level.[43] The concept of privacy is simply too contextual and vague to meaningfully direct the relevant stakeholders in design-based decisions to protect Internet users. Instead, this Article proposes that general design principles to protect users of social technologies should be based on the concept of obscurity. The following section explores the concept of online obscurity, summarizing our own research and that of others on the topic, and why obscurity is the ideal front-end design principle for online communication technologies like social network sites.

A. The Concept of Obscurity

Obscurity is defined as a state of unknowing.[44] If an individual is obscure, this means that an observer does not possess critical information that allows them to make sense *of* the individual. This critical information can include the individual's identity, social connections, and other personal information. Without this information, observers are limited in their ability to fully comprehend an observed person's actions and utterances. Employees on a lunch break in a restaurant often gossip about their co-workers, but this gossip is obscure to eavesdroppers unless these outsiders know the subject of the gossip; those in earshot must be able to draw on unspoken contextual information to make sense of the utterances. This information enables what Erving Goffman has referred to as "presupposition."[45] Though we colloquially say we socialize in "public," in truth our personal interactions are usually enveloped in zones of obscurity, where our identity and personal context are shielded to those we interact or share common space with.

Social media users also have come to rely upon obscurity for privacy protection online. Obscurity is a natural state offline that users can draw upon reflexively when protecting their privacy in online social settings.[46]

Guidelines, NATION, http://www.thenation.com/community-guidelines (last visited Apr. 17, 2013).

43. *See, e.g.*, Gelman, *supra* note 4; Grimmelmann, *supra* note 4; Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

44. Hartzog & Stutzman, *Online Obscurity*, *supra* note 9, at 5.

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

46. *See, e.g.*, IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL

For example, the mere act of disclosing information online does not necessarily mean that the individual seeks wide publicity, even if the information disclosed is theoretically available to the Internet at large. Just as an individual shouting from the street corner will only be heard by so many individuals (her audience is limited by architecture, social interaction, and pure physics), the rational online discloser has similar expectations with content shared online.[47]

The choice to disclose online involves a highly contextual cost/benefit analysis.[48] Individuals control the information disclosed online by limiting the audience of the disclosure, by limiting the meaning of the disclosure, and by adapting the disclosure to a particular website.[49] Because anonymity would violate norms and limit benefits attained from many social network sites such as Facebook, individuals instead develop techniques that effectively produce obscurity in disclosure.[50] As obscurity is a protective, privacy-enhancing state where we are guarded by an observer's inability to completely comprehend our action, it is particularly useful to users of social media tools.

Contrary to the powerful popular discourse that argues that

SPACE, TERRITORY, AND CROWDING (1975); SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE (2002).

47. For example, numerous papers have documented the characteristics of the "attention economy" online, where a multitude of information producers compete furiously for limited attention. To attain large-scale attention requires the expense of significant resources; individuals who do not seek, or seek limited, publicity have very good reason to expect obscurity. *See, e.g.*, MARK NEWMAN, ALBERT-LÁSZLÓ BARABÁSI & DUNCAN J. WATTS, THE STRUCTURE AND DYNAMICS OF NETWORKS (2006); Jon M. Kleinberg, *Authoritative Sources in a Hyperlinked Environment*, 46 J. ASS'N COMPUTING MACHINERY 604 (1999).

48. *See, e.g.*, Joseph B. Walther, *Selective Self-Presentation in Computer-Mediated Communication: Hyperpersonal Dimensions of Technology, Language, and Cognition*, 23 COMPUTERS HUM. BEHAVIOR 2538 (2007).

49. *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.asp.; 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; Stutzman and Hartzog, *Online Obscurity*, *supra* note 9, at 16; Martin Tanis & Tom Postmes, *Social Cues and Impression Formation in CMC*, 53 J. COMM. 676 (2003).

50. *See* 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; Stutzman & Hartzog, *Boundary Regulation*, *supra* note 9; *see also* 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.

individuals online have essentially different privacy and notoriety goals, our previous work "demonstrate[d] that online obscurity is a crucial aspect of privacy for Internet users."[51] Through obfuscation techniques and other normative user practices, it is clear that obscurity is both desired and expected online. "Internet users routinely hide information by making it invisible to search engines, using pseudonyms and multiple profiles, and taking advantage of privacy settings."[52] In short, users *produce* obscurity online. Thus, obscurity is the ideal locus for design-based solutions that empower users to produce and exist in their own privacy protective contexts.

B. The Four Principles of Online Obscurity

Our previous research has offered a clear definition of online obscurity: "Information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We have identified four of these factors: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity. The presence of these factors diminishes obscurity, and their absence enhances it."[53] This Part summarizes that conceptualization with an eye toward design.

Information can be plotted on a spectrum of obscurity that will allow regulators, designers, and organizational stakeholders to adopt guiding principles regarding the protection of online information. The aim of obscurity, as opposed to the broader and more intractable goal of "privacy," would provide policymakers and organizational stakeholders with a more nuanced set of "starting points" that could be applied flexibly via design-based solutions across culture and context. We now consider how each of the four factors of obscurity can be approached through design.

1. Search Visibility

Search visibility is the degree to which individuals and the content they produce are locatable and accessible through search.[54] Search invisibility is one of the most significant factors in online obscurity because it is the primary method for discovering online information.[55]

---

51. Hartzog & Stutzman, *Online Obscurity*, *supra* note 9, at 16.

52. *Id.* at 2.

53. *Id.* at 48.

54. *See id.* at 35–36.

55. *See, e.g.*, DEBORAH FALLOWS, PEW INTERNET & AM. LIFE PROJECT, SEARCH ENGINE USE (2008), *available at* http://www.pewinternet.org/Reports/2008/Search-Engine-Use/Data-

Without search, information can only be discovered in less efficient ways such as a chain-hyperlink fashion via other websites, messages, and manual URL entry.

In many ways, search invisibility is already the default for most online information.[56] Search invisibility can be achieved by intentionally shielding websites from search engines using the robot.txt file as well as by using privacy settings or other access restrictions such as passwords, which are another factor in online obscurity.[57] Because search is a primary and common vector for discovery of individual content, designers should consider offering controls over inclusion in both internal and external search services. For example, some people may want their profile to appear in Google, while others would prefer only to

---

Memo.aspx; SUSANNA FOX, PEW INTERNET & AM. LIFE PROJECT, SEARCH ENGINES (2002), *available at* http://www.pewinternet.org/Reports/2002/Search-Engines/Data-Memo.aspx; LEE RAINE, PEW INTERNET & AM. LIFE PROJECT, BIG JUMP IN SEARCH ENGINE USE (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); Jamie Teevan, Susan T. Dumais & Eric Horvitz, *Potential for Personalization*, 17 ACM TRANSACTIONS ON COMPUTER-HUM. INTERACTION 1 (2010).

56. This information, collectively known as "the dark Web," "the deep Web" or "the invisible Web," accounts for 80-99% of the World Wide Web. *See, e.g.*, MICHAEL K. BERGMAN, THE DEEP WEB: SURFACING HIDDEN VALUE (2001), *available at* http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104 ("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. & SERV. 18 (2002); Yanbo Ru & Ellis Horowitz, *Indexing the Invisible Web: A Survey*, 29 ONLINE INFO. REV. 249 (2005); Andy Beckett, *The Dark Side of the Internet*, GUARDIAN (Nov. 25, 2009), http://www.guardian.co.uk/technology/2009/nov/26/dark-side-internet-freenet; 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. 15, 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).

57. 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.COM, http://www.google.com/support/blogger/bin/answer.py?hl=en&answer=41373 (last visited Apr. 27, 2011). Facebook profiles that utilize privacy settings are also not found by search engines. *See How Can I Control if Other Search Engines can Link to My Timeline?*, FACEBOOK, http://www.facebook.com/help/392235220834308/ (last visited May 6, 2011); *see also* Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 102 (2008) ("Today, nearly all Web programmers know robots.txt is the way in which sites can signal their intentions to robots, and these intentions are voluntarily respected by every major search engine across differing cultures and legal jurisdictions.").

be "searchable" one or two network degrees out (e.g., by friends-of-friends). Designers may also consider offering various levels of search engine obfuscation, where only certain aspects of the profile are placed into search, or search placement is manipulated to raise or lower placement of results. Design options are discussed in greater detail in Part III below.

2. Unprotected Access

Access protection covers a range of technologies and methods for controlling access to content.[58] A common example of an access control is the password. Access controls can serve multiple functions apart from merely technologically restricting who can view information. Access controls can also serve as normative signals indicating the private nature of the information. Conversely, unfettered access to information, particularly when technologies like privacy settings are available but unused, can have the opposite effect on obscurity, leaving the information exposed and subject to being scraped, indexed, and aggregated.

There are many different kinds of access controls, including biometrics, encryption, privacy settings, and passwords. These controls can provide for user control over several variables, including the content shared, the specifics of the potential audience, or both. As ubiquitous computing systems change and adoption increases, dynamically generated access controls are likely to evolve—controls that are reactive to the environment and its network configurations.[59] Along with search visibility, access controls are one of the most important factors to create online obscurity. Consequently, they should be considered bedrock tools for designers embracing the principals of obscurity.

3. Identification

Identification refers to the degree that individuals are identified through personal and interpersonal disclosures in online settings. Identification is defined here as the existence of an irrefutable piece of information that links content online to the individual's person.

---

58. *See* Hartzog & Stutzman, *supra* note 9, at 37–38.

59. *See, e.g.*, Giovanni Iachello & Jason Hong, *End-User Privacy in Human-Computer Interaction*, 1 FOUNDS. & TRENDS 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.

Information that cannot be linked to a person offers a degree of anonymity and poses a reduced threat to that person's privacy.[60] While many PETs and other design strategies focus on anonymity,[61] obscurity is much more concerned with the use of pseudonyms and ID variants given their utility in socialization. Like passwords, ID variants and pseudonyms can somewhat protectively de-link content and identity. Readily apparent ID variants and pseudonym can also signal to the recipient of information that the identity of the discloser is sensitive or private.

Social technologies present multiple challenges to identity management. For example, on social network sites, where the articulation of the social network is a key feature, identification can occur through both direct and indirect disclosures.[62] Users maintaining a pseudonymous profile may become publicly identifiable based on whom the individual connects to, or what a friend writes on the individual's wall.[63] Therefore, designers should be aware that the individual's intention to protect her or his identity extends beyond self-disclosure to managing disclosures about the individual and selective crafting of the online persona.

4. Clarity

Finally, clarity covers the degree to which an outside observer can make sense of content shared by an individual.[64] Often, online information is easily discoverable, but important aspects of that information do not make sense to the reader or viewer.[65] Sometimes this information is intentionally vague or incomplete. Information in one domain might be separated by medium, tool, or linkage from another piece in order to make it more obscure, and, thus, more protected.[66] If information is too vague or incomplete to understand, it lacks clarity.[67]

---

60. *See* Iachello & Hong, *supra* note 59, at 2–3.

61. *See, e.g.*, Rubinstein, *supra* note 6, at 1411, 1415.

62. *See* J. Donath & d. boyd, *Public Displays of Connection*, 22 BT TECH. J. 71 (2004).

63. *See, e.g.*, Arvind Narayanan & Vitaly Shmatikov, Remarks at the 30th IEEE Symposium on Security and Privacy: De-anonymizing Social Networks (May 17–20 2009), *in* 2009 IEEE SYMPOSIUM ON SEC. & PRIVACY, 2009, at 173–87 (abstract available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5207644&isnumber=5207632).

64. *See* Hartzog & Stutzman, *Online Obscurity*, *supra* note 9, at 39.

65. *See id.*

66. *See, e.g.*, Stutzman & Hartzog, *Boundary Regulation*, *supra* note 9.

67. *See Clarity Definition*, MACMILLAN DICTIONARY, http://www.macmillandictionary.com/dictionary/american/clarity#clarity_3 (last visited May 30, 2013).

Whereas the identification factor of obscurity focuses on the link between identity and information, clarity focuses on the link between content and some other contextual factor. Stripping context from information reduces its clarity and increases the obscurity of information by reducing the number of people who are likely to understand the meaning of the disclosure. This technique is common in our everyday social interactions. Groups that are familiar with each other can "presuppose" contexts in conversation, instead of explicitly providing for it with each disclosure.[68] In our previous research, we conceptualized "clarity" as the "range of shared social, cultural, and linguistic factors that enable presupposition."[69] The previously mentioned eavesdroppers on gossip may be able to understand some of what is spoken aloud, but there will likely be a lack of clarity that prohibits true comprehension or identification of the conversational subjects. The same can be said for communication via social technologies, which is often clouded by in-group presuppositions that inhibit clarity.[70]

Designers can approach clarity by both recognizing and valuing individual strategies for managing clarity (i.e., respecting this normative practice in both policy and technology), and by considering the degree to which meta-data, data stores, and data recombination allows outside individuals to programmatically construct clarity of observed information.[71] Such considerations are especially important given the risks to persons (e.g., job security, safety) that can emerge from inadvertent disclosures.

Obscurity is capable of being easier to refine and implement than the broader concept of privacy. Where the pursuit of "privacy" in design often seems like a quest for near-perfect protection, the goal of designing for obscurity is that it be *good enough* for most contexts or a user's specific needs**.** Protection is achieved via obscurity not necessarily through the strength of the "armor," but rather, through a significant reduction in the probability of discovering or understanding information. Obscurity is a more nuanced and accurate reflection of the expectations of users of social technologies than the broader, and potentially misleading, concept of privacy.[72]

---

68. Goffman, *supra* note 45, at 1.

69. Hartzog & Stutzman, *Online Obscurity*, *supra* note 9, at 39.

70. *See, e.g.*, Tanis & Postmes, *supra* note 49; Walther, *supra* note 48.

71. *See, e.g.*, Alessandro Acquisti, Ralph Gross & Fred Stutzman, Privacy in an Age of Augmented Reality (unpublished manuscript) (on file with authors).

72. *See* Hartzog & Stutzman, *Online Obscurity*, *supra* note 9, at 31–40.

III. IMPLEMENTING OBSCURITY BY DESIGN

This Article has proposed that obscurity is the natural state for most online social communications and, as such, should be the locus of design-based privacy solutions for social technologies. This part explores how the various organizational stakeholders can work together to create a model of "obscurity by design" for social technologies. Specifically, this part explores ways to implement obscurity by design through technologies, policies, and behavioral interventions. These implementations would enable and encourage users to create or maintain a context of obscurity.

It is important to note the role of design and designers within this conceptualization. Those actually tasked with the nuts and bolts of assembling social technologies, such as product managers, designers, and software engineers, will be crucial in designing for obscurity. Given obscurity by design's focus on the "front end" or user interface of social technologies, these design teams will play an extremely important role in implementing policy goals.

But a successful scheme of privacy by design must include all of the relevant stakeholders in an organization, including the legal counsel who drafts a technology's terms of use and privacy policy, and the higher-level decision makers who set the goals and basic parameters of the technology. While different organizational stakeholders might claim responsibility for the ultimate implementation of various technologies, policies, and nudges, a true obscurity by design approach should attempt to bring together all of the organizational stakeholders to coordinate the implementation process. Indeed, complete organizational responsibility is one of the central tenets of privacy by design.[73]

Of course, obscurity is not the only desired goal of privacy protection in social technologies. Some communication, like information on publicity-seeking blogs and some Twitter accounts, need little protection and are unlikely to be viewed as private or obscure in most instances. Obscurity would actually be a hindrance to those seeking widespread publicity.[74] Other communications, such as sensitive health information and extremely intimate disclosures about personal relationships, would likely require more protection than obscurity, and thus the desired level

---

73. *See* Cavoukian, *Privacy by Design*, *supra* note 1, at 1.

74. For those seeking to make a living by writing and publishing information, obscurity is actually an obstacle to overcome. *See, e.g.*, CORY DOCTOROW, THE PROBLEM ISN'T PIRACY, THE PROBLEM IS OBSCURITY (Children's Book Insider ed., 2011), *available at* http://www.write4kids.com/blog/wp-content/uploads/2011/05/doctorow.pdf.

of protection should be confidentiality or secrecy.[75] Optimally, users should be able to adjust their level of protection from the obscurity default to achieve either more publicity or greater confidentiality or secrecy.

Indeed, many of the proposals to implement obscurity by design can also serve the interests of the more protective concepts of confidentiality or secrecy. Alternatively, some of these proposals can also serve as a transitional tool that helps ensure a gradual, controlled, and layered approach to publicity, rather than a meteoric ascent into fame—metaphorical speed bumps for online communication. Thus, these proposals are pliable and capable of effectuating a number of different policy goals.

A. Technologies

Perhaps the most obvious way to design for obscurity is to create technologies that directly produce obscurity or enable users to produce obscurity for themselves. These technologies can include, but are not limited to, PETs such as the option to hide individual content from internal and external search engines.[76] In social media, friendship, follower status, or group status generally govern access. In blogs or websites, either credentials (such as passwords) or encryption govern access. Following this logic, smart hyperlinks and privacy settings could restrict access to various degrees and, by doing so, raise the transactional cost of finding information and making that information more obscure. Such high costs decrease the likelihood that information will be found and used in harmful ways.

1. Smart Hyperlinks and Access Walls

Consider the case where an individual would like to semi-privately share content without passwords or social network connections. Through the use of cookies, a "paywall"-like technology could be designed to only accept links from certain sources restricting access to content.[77] For example, a link might not lead to the correct page unless the user clicked

---

75. *See, e.g.*, Woodrow Hartzog, *The Privacy Box: A Software Proposal*, FIRST MONDAY (Nov. 2, 2009), http://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/2682/2361.

76. *See, e.g.*, Spiekermann & Cranor, *supra* note 36.

77. Of course, paywall technologies are both controversial and subject to circumvention. But increasing the labor required to access information is another way to lower the probability of discovery. *See, e.g.*, Tim Brookes, *5 Ways to Get Around the New York Times Paywall*, MAKEUSEOF (Mar. 30, 2011), http://www.makeuseof.com/tag/5-ways-york-times-paywall/.

it while within a protected online community or if certain cookies existed on the user's computer authorizing the disclosure.[78] Alternatively, the link might work only when the web server can confirm that the link is embedded within a certain webpage.

These "smart hyperlinks" could help ensure that only members of the protected community or other verified users could access the information. Additionally, these links would help maintain the obscurity of information by frustrating the ease of dissemination online.[79] Most links are easily shared through being cut and pasted into e-mails or social media postings. These smart links would require the extra step of manually disseminating the information itself, rather than the hyperlink. While such a technique might not adequately protect confidential or secret information, it would likely help obscure information by reducing the number of people likely to disseminate it.[80] While not perfect, this flexible approach could meaningfully help enable selective disclosure.

2. "Privacy" Settings

Some of the most common tools to help users produce obscurity are privacy settings.[81] These settings, which generally allow Internet users to control the potential audience of their disclosures on a website, are often criticized as not protecting privacy at all because hundreds, if not thousands, can regularly still have access to "protected" disclosures.[82] This critique highlights the problems with relying upon conceptualizations of privacy to guide design.

---

78. It should be noted that there are privacy implications regarding the use of cookies, but these threats are better addressed by other strategies within privacy by design and are beyond the scope of this Article. *See, e.g.*, Ashkan Soltani et al., *Flash Cookies and Privacy* (University of California, Berkley, Working Paper, Aug. 10, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862; Joseph Turow et al., *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Working Paper, Sep. 29, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

79. *See* Hartzog & Stutzman, *Online Obscurity*, *supra* note 9.

80. *See, e.g.*, Strahilevitz, *supra* note 43.

81. MARY MADDEN & AARON SMITH, PEW INTERNET & AM. LIFE PROJECT, REPUTATION MANAGEMENT AND SOCIAL MEDIA 29 (2010), *available at* http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx (finding that "[n]early three quarters (71%) of social networking users ages 18-29 have changed the privacy settings on their profile to limit what they share with others online").

82. *See, e.g.*, Loporcaro v. City of New York, No. 100406/10, 2012 WL 1231021, at *7 (N.Y. Sup. Ct. Apr. 9, 2012) ("When a person creates a Facebook account, he or she may be found to have consented to the possibility that personal information might be shared with others, notwithstanding his or her privacy settings, as there is no guarantee that the pictures and information posted thereon, whether personal or not, will not be further broadcast and made available to other members of the public.").

These technologies are likely better understood as "obscurity settings." They help the user hide from search engines and control who accesses their personal information, two of the most important factors of our conceptualization of online obscurity. Previous research supports the assertion that Internet users utilize privacy settings for numerous reasons such as propriety, audience management, and obscurity.[83] These settings can serve as bedrock technologies to enable obscurity and would likely be a staple for obscurity by design for social technologies.

3. Search Blockers

Because one of the main factors that enables obscurity is search invisibility, technologies that keep websites from being indexed by search engines are highly effective ways to design for obscurity. Previously discussed technologies such as password systems, privacy settings, and paywall-like technologies serve dual purposes of restricting access as well as keeping certain pieces of information from being cataloged by search engines.[84]

However, other technologies can also serve this function. The robot.txt file[85] is a simple and effective way for websites to indicate non-participation in search engines.[86] Search invisibility can be woven into the design of social technologies. For example, the popular blog creation tool Tumblr, allows users to hide their blogs from search engines.[87] On the settings page for any particular blog, users can reverse this result by checking a box to indicate the user's desire to "[a]llow search engines to index your blog."[88]

Designers might also consider offering various levels of search engine obfuscation, where only certain aspects of a profile or website are placed into search. Designers could make information searchable only at the

---

83. *See, e.g.*, Stutzman & Hartzog, *Boundary Regulation*, *supra* note 9.

84. *See* Hartzog & Stutzman, *Online Obscurity*, *supra* note 9.

85. According to Google, "A robots.txt file restricts access to your site by search engine robots that crawl the web. These bots are automated, and before they access pages of a site, they check to see if a robots.txt file exists that prevents them from accessing certain pages." *Block or Remove Pages Using a Robot.txt File*, GOOGLE.COM, http://support.google.com/webmasters/bin/answer.py?hl=en&answer=156449 (last visited Apr. 25, 2013).

86. *See, e.g.*, Zittrain, *supra* note 57, 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.").

87. *See, e.g.*, Ashley Poland, *Can You Restrict Ages on Tumblr?*, EHOW (June 29, 2011), http://www.ehow.com/info_8665566_can-restrict-ages-tumblr.html.

88. *Id.*

site level but remain invisible to general search engines. Search engine optimization techniques could be inverted to lower the placement of certain results, a sort of search engine diminishment. Any combination of technology and strategy to diminish or erase search engine visibility of information would count as a valid implementation of obscurity by design.

4. De-Identifying Tools

Facial recognition technology is evolving rapidly.[89] It is only a matter of time before individuals in photographs and videos online can be automatically identified.[90] "Augmented reality," that is, "a live, direct or indirect, view of a physical, real-world environment whose elements are augmented by computer-generated sensory input such as sound, video, graphics or GPS data," will continue to find its way into social technologies.[91] The identities of individuals in online media are often obscure because they are not included in the search results for the individuals' names. *Post hoc* identification of these individuals would destroy the obscurity they enjoyed with regard to these videos and images. Thus, any technology that frustrated facial recognition and other identification tools would effectuate obscurity by design.

For example, Google has announced plans to implement a technology that allows users to blur the faces of those appearing in videos before posting them to YouTube.[92] The tool has been envisioned as another option for dealing with privacy complaints submitted by people depicted in another user's videos. In addition to the more severe consequence of video deletion due to privacy complaints, video creators will also have the option to blur the complainant's face, which will allow the videos to remain on YouTube.[93]

While face-blurring might still leave individuals subject to identification in some contexts, this technique could have two positive

89. *See, e.g.*, Megan Geuss, *Facebook Facial Recognition: Its Quiet Rise and Dangerous Future*, PCWORLD (Apr. 26, 2011), http://www.pcworld.com/article/226228/Facerec.html.

90. *See id.*; Acquisti et al., *supra* note 71; Sarah Jacobsson Purewal, *Why Facebook's Facial Recognition is Creepy*, PCWORLD (June 8, 2011), http://www.pcworld.com/article/229742/why_facebooks_facial_recognition_is_creepy.html.

91. *Augmented Reality*, MASHABLE, http://mashable.com/follow/topics/augmented-reality/ (last visited May 1, 2012); *see also* Scott R. Peppet, *Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts*, 59 UCLA L. REV. 676 (2012).

92. *See* Thomas Claburn, *YouTube Tool Blurs Faces to Protect Privacy*, INFO. WEEK (Mar. 29, 2012), http://www.informationweek.com/news/security/privacy/232700524.

93. *Id.*

outcomes for obscurity: (1) only those with external knowledge of individuals with blurred faces would likely be able to identify them, effectively protecting the individual from recognition by most strangers, and (2) blurred faces will frustrate facial recognition technologies. As such, these technologies would help implement obscurity by design.

5. Passwords and Encryption

Some technologies, such as password systems and encryption, can clearly obscure disclosures because these tools can significantly restrict outsider access and thus raise the transactional cost of finding information. Indeed, these technologies can often protect more than the obscurity of information—they can keep information a secret that is unknown or unseen by others. While designers should always be willing to consider these powerful tools, they should be mindful regarding their implementation for the front end of social technologies (as opposed to back-end or in-transit uses like "https" or encrypting electronic messages, which are important aspects of privacy by design).[94] Too many restrictions on the accessibility of disclosures might unduly inhibit social interaction and frustrate the purpose of the technology.

B. Policies

Not all technology design decisions relate to the creation and implementation of tools. The creation and protection of obscurity can also be facilitated by rules that explicitly allow or discourage certain behavior. Terms of use and policies can allow users to create their own obscurity, for example by using a pseudonym, as well as prevent other social technology users from engaging in obscurity-eroding behavior, such as scraping data from websites. These policies generally fall into two categories: behavioral restrictions, which are largely imposed to govern the user's behavior in relation to the technology, and community guidelines, which are imposed as the "rules of the road" between users within an online community.

1. Contractual Restrictions on User Behavior

Terms of use agreements in technologies like social media commonly

---

94. *See, e.g.*, Alexis C. Madrigal, *A Privacy Manifesto in Code: What if Your Emails Never Went to Gmail and Twitter Couldn't See Your Tweets?*, ATLANTIC (Apr. 4, 2012), http://www.theatlantic.com/technology/archive/12/04/a-privacy-manifesto-in-code-what-if-your-emails-never-went-to-gmail-and-twitter-couldnt-see-your-tweets/255414/.

include restrictions on user behavior. These restrictions, such as prohibitions on scraping data and requesting one's user name and password, can prevent other individuals (and bots) from diminishing a technology user's obscurity. Other policies, such as the requirement that social media users list their real name, can frustrate a user's obscurity protections. Policies that discourage activities that erode obscurity and encourage obscurity-friendly behavior should be considered an implementation of obscurity by design. Because lack of identification is a major factor in online obscurity, designers should construct policies and technologies that allow for pseudonyms, name variants, and/or the use of multiple profiles to represent multiple facets of identity. Indeed, Google+, the search giant's social media platform, has already modified its terms to allow the use of some pseudonyms.[95] This development occurred as part of the so-called "nym-wars," which brought attention to the importance of pseudonymity.[96] Other social network sites have "real name" policies that require strong identification of site members through norms, and sometimes through enforcement action.[97] These policies are controversial as the requirement of real names can disenfranchise a wide range of users (e.g., victims of abuse, political opposition) who face threats if they speak publicly with their "real names."[98] Some users simply want to bifurcate their online identity by creating two different social media profiles.[99] Multiple profiles produce obscurity by de-linking aspects of an individual's identity. Yet this practice is also prohibited by some social network websites, including Facebook.[100] Real name policies and prohibitions on multiple profiles can help verify one's online identity, but these practices significantly diminish obscurity by

---

95. *See* Eva Galperin, *Google+ and Pseudonyms: A Step in the Right Direction, Not the End of the Road*, ELECTRONIC FRONTIER FOUND. (Jan. 24, 2011), https://www.eff.org/deeplinks/2012/01/google-pseudonyms-step-right-direction-not-end-road.

96. *See* Eva Galperin, *2011 in Review: Nymwars*, ELECTRONIC FRONTIER FOUND. (Dec. 26, 2011), https://www.eff.org/deeplinks/2011/12/2011-review-nymwars.

97. *See Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/terms.php?ref=pf (last visited Apr. 26, 2011) [hereinafter *Statement of Rights*] ("Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account: . . . You will not provide any false personal information on Facebook . . . .").

98. *See* Jillian C. York, *A Case for Pseudonyms*, ELECTRONIC FRONTIER FOUND. (July 29, 2011), https://www.eff.org/deeplinks/2011/07/case-pseudonyms.

99. *See, e.g.*, Stutzman and Hartzog, *Boundary Regulation*, *supra* note 9 (finding that users often use multiple profiles for "personal" and "professional" separation).

100. *Statement of Rights*, *supra* note 97 ("Here are some commitments you make to us relating to registering and maintaining the security of your account: . . . You will not create more than one personal account.").

design.

Restrictions on revealing one's username and password can also help create obscurity, as well as security, by functioning as a non-technological burden on accessing information. One of the easier ways of accessing a user's social media profile is to do so directly via requests for one's username and password. Third-party requests for social media user's passwords are seemingly on the rise.[101] However, as part of the registration process, Facebook and other social network sites require promises such as "[y]ou will not share your password . . . let anyone else access your account, or do anything else that might jeopardize the security of your account."[102]

Designers can protect the obscurity of their users' information by prohibiting scraping.[103] In the obscurity context, scraping restrictions are a form of access control against automated information harvesting.[104] Essentially, these restrictions mandate that, for most purposes, only humans can access online information, as opposed to bots. This restriction helps produce obscurity by limiting the aggregation and further dissemination to "manual" methods, which are more time consuming and less likely to present systematic risks to privacy. Information harvesting typically results in aggregation of information, which associates information that was previously separate. This separation prevented certain kinds of presupposition crucial to understanding individuals and information.[105] In other words,

---

101. For example, in September 2007, a cheerleading coach at Pearl High School in Mississippi allegedly required the members of her cheerleading squad to reveal the usernames and passwords of their Facebook accounts. Brian Stewart, *Student Files Lawsuit After Coach Distributed Private Facebook Content*, STUDENT PRESS L. CENTER (July 22, 2009), http://www.splc.org/newsflash.asp?id=1938; *cf.* David L. Hudson, Jr., *Site Unseen: Schools, Bosses Barred from Eyeing Students', Workers' Social Media*, A.B.A. J. (Nov. 1, 2012, 3:10 AM), http://www.abajournal.com/magazine/article/site_unseen_schools_bosses_barred_from_eyeing_students_workers_social_media.

102. *Statement of Rights*, *supra* note 97.

103. *See, e.g.*, *id.* ("You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.").

104. Automated information harvesting by third parties also threatens individuals' obscurity and is typically governed via terms of use. *See* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) ("Many webpages contain lengthy limiting conditions, including limitations on the use of scrapers."). "Web Scraping is the process of taking html or data from the web and organizing that data into an organized format . . . . Common uses for web scraping is the gathering and retrieval of large amounts of information that would be to unwieldy to gather by hand." *Web Scraping Definition*, EXTRACTINGDATA.COM, http://www.extractingdata.com/web%20scraping.htm (last visited Aug. 10, 2010).

105. *See, e.g.*, Goffman, *supra* note 45.

aggregating information can often clarify it, which makes that information more obvious and less obscure.

A number of social technologies have already incorporated this design principle. Facebook mandates that visitors "will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission."[106] It goes on to state that "[i]f you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it."[107]

2. Community Guidelines

While "behavior restrictions" provide rules for the relationship between the user and the website, terms of use agreements and website policies also have the opportunity to serve as a mediator of conduct between the users of online communities. These "rules of the road" for online social interaction are often called "community guidelines,"[108] and—in addition to contractually restricting behavior—they can potentially help set the normative expectations for online communities.

These rules of the road need not be in the terms of use agreement to be effective from a design perspective. Indeed, because virtually nobody reads the terms of use, inserting community guidelines into boilerplate will all but assure their ineffectiveness.[109] Instead, these guidelines should be made prominent at the point of disclosure to gently remind members of the community of what the normatively expected behavior is. For example, a small textual box next to a status-posting tool in a social network site might incorporate language from the website's terms of use, such as, "Remember, this is a community that relies upon discretion" or "Let's keep what we learn here between members of the

106. *Statement of Rights*, *supra* note 97.

107. *Id.*

108. *See, e.g.*, *Flickr Community Guidelines*, FLICKR, http://www.flickr.com/help/guidelines/ (last visited May 1, 2012); *MySpace.com Terms of Use Agreement*, MYSPACE, http://www.myspace.com/Help/Terms?pm_cmp=ed_footer (last visited June 25, 2009); *The Twitter Rules*, TWITTER, https://support.twitter.com/articles/18311-the-twitter-rules (last visited May 1, 2012); *YouTube Community Guidelines*, YOUTUBE, http://www.youtube.com/t/community_guidelines (last visited May 1, 2012) ("We're not asking for the kind of respect reserved for nuns, the elderly, and brain surgeons. We mean don't abuse the site. Every cool new community feature on YouTube involves a certain level of trust. We trust you to be responsible, and millions of users respect that trust. Please be one of them.").

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

community."

Community guidelines should not be in legalese. They should be short and easy to understand.[110] Designers could experiment with various levels of formality and injunctions of humor to determine the most effective way to inform users of the rules. Designers also have the option of implementing the guidelines normatively or incorporating them into their terms of use as part of a contractually binding agreement.

For example, the online photo community of Flickr provides very simple community guidelines, many of which enhance obscurity.[111] Under "What *not* to do," Flickr reminds users, "Don't forget the children," saying "If you would hesitate to show your photos or videos to a child, your mum, or Uncle Bob, that means you need to set the appropriate content filter setting. If you don't, your account will be moderated and possibly deleted by Flickr staff."[112] The content filter is a technological control that can affect access and is a great way to blend design tools to create obscurity. The website also uses humor to enforce civility and respect for the community, stating, "Don't be creepy. You know the guy. Don't be that guy."[113]

C. Behavioral Interventions

Modern behavioral economics and social psychology have demonstrated that small design decisions can have a significant impact on an individual's behavior.[114] To effectuate obscurity by design, we recommend drawing from these disciplines to provide instruction on how, in the parlance of Richard Thaler and Cass Sunstein, to "nudge" users toward obscurity-friendly practices.[115] We refer to design decisions made to encourage obscurity-friendly practices as behavioral interventions.

---

110. *Cf.* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J. L. & POL'Y FOR INFO. SOC'Y 543 (2008).

111. *See Flickr Community Guidelines*, *supra* note 108.

112. *Id.*

113. *Id.*

114. *See, e.g.*, DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011); CHOICES, VALUES, AND FRAMES (Daniel Kahneman & Amos Tverskey, eds., 2000); *see also* Ryan Calo, Code, Nudge, or Notice? (Feb. 7, 2013) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2217013.

115. RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008). Thaler and Sunstein conceptualize a "nudge" as "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates." *Id.*

These behavioral interventions could work in tandem with or in place of technologies and policies to gently enhance user obscurity in social technologies without mandating conduct or precluding certain kinds of activity. It is important to emphasize that, consistent with the thesis of this Article, these interventions are offered not as excessive protections to limit user behavior, but rather as clarifications and corrective measures that help users understand and effectuate the true and desired state of their online communications.

1. Defaults

There may be no more central tenet to obscurity by design and privacy by design as a whole than the importance of privacy-friendly default settings.[116] Indeed, the issue of defaults for consumers and technology users is important in other areas of privacy law.[117] The reason why the default setting is such a critical design decision is that individuals will usually stick with whatever the default choice is, even when the default is less advantageous or more harmful than the non-default options.[118] This power of inertia and general reluctance of individuals to alter default choices has been called "status quo bias."[119] Default settings can even be seen as an implicit endorsement from the default setter that the settings are desirable.[120] Thus, it is extremely important to consider the proper default setting for social technologies and implement the most responsible choice.

We have argued that, for most social technologies, obscurity is the natural context for the disclosure of personal information. Consequently, any organization seeking to adhere to the principles of obscurity by design should set their default choices for users in the most obscurity-friendly way available. For example, if a social technology offers privacy settings, the settings should, at a minimum, default to render

---

116. *See* CAVOUKIAN, PRIVACY BY DESIGN, *supra* note 1; CAVOUKIAN, SEVEN FOUNDATIONAL PRINCIPLES, *supra* note 1.

116. *See* FTC, PROTECTING CONSUMER PRIVACY, *supra* note 2.

117. *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

118. THALER & SUNSTEIN, *supra* note 115, at 8.

119. William Samuelson & Richard Zeckhauser, *Status Quo Bias in Decision Making*, 1 J. RISK & UNCERTAINTY 7 (1988).

120. Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 603 (2006) ("[P]eople believe defaults convey information on how people should act.").

disclosures invisible from search and limit other user's access in some significant way (i.e., not offer unfettered access).

2. Feedback

Designing feedback mechanisms into social technologies might be one of the most powerful behavioral interventions available to implement obscurity by design. Feedback can be effective for a number of reasons, including helping make risks more salient and appealing to individuals' desire for conformity.[121]

One kind of feedback that might be effective for designers could be a form of what Professor Ryan Calo calls "visceral notice," notice that is visceral "in the sense of changing the consumers understanding by leveraging the very experience of a product or service."[122] Feedback could be categorized as "showing," or "tailoring notice very specifically to the company's engagement with the exact individual."[123] Calo states "[t]echnology and clever design create the possibility of tailoring anecdotes to individual consumers, thereby showing them what is specifically relevant to them, instead of describing generally what might be."[124]

As an example, Calo describes how Mozilla, the designer of the popular Firefox browser, "shows" users their privacy practices by providing the user feedback on what information is collected by the browser.

Consistent with standard legal practice, Mozilla provides a

---

121. *See, e.g.*, Dan M. Kahan, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. CHI. L. REV. 607, 613 (2000) ("The tendency of individuals to conform—a phenomenon psychologists call 'social influence'—is pervasive: diners prefer to patronize the restaurants that they think other diners will patronize, and citizens to vote for the candidates for whom they think others will vote; teenage girls are more likely to become pregnant when they see that others are having babies, and adults more likely to go on welfare when they become acquainted with others who are on the dole."); Jonathan Klick and Gregory Mitchell, *Government Regulation of Irrationality: Moral and Cognitive Hazards*, 90 MINN. L. REV. 1620, 1629 (2006) ("The main vehicle to greater decision-making competence is alteration in existing psychological states such that later psychological states possess more reliable knowledge about what ends are most valued and how best to achieve those ends. Outcome feedback and verbal feedback serve as the main mechanisms for change between earlier and later psychological states.").

122. M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1033 (2012).

123. *Id.* at 1042. For preliminary results regarding an experiment that measures, among other things, "showing" as a notice technique, see Victoria Groom & M. Ryan Calo, Reversing the Privacy Paradox: An Experimental Study (Sept. 25, 2011) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1993125.

124. Calo, *supra* note 122, at 1042.

> privacy policy and terms of use that explain, generally, what information Mozilla might collect and how it might use that information. About one study, Mozilla says: "We will periodically collect data on the browser's basic performance for one week . . . ." Prior to transmitting user information from the user's computer to Mozilla's servers, however, Mozilla also shows users a report of what information has actually been collected and asks them to review and approve it. Thus, users actually see a specific, relevant instance of collection and decide to consent on this basis.[125]

Calo concludes, "Executed well, showing describes what has actually occurred, thereby embedding information about the company's practices in the consumer experience of the produce or service—similar to the way we might best learn the rules of a game by playing it."[126]

Social technologies provide abundant opportunities for feedback through "showing" users aspects of their social network or interactivity that might encourage obscurity-friendly practices. For example, showing users the size of their potential audience or five randomly selected "friends" at the point of disclosure might help users better understand the scope of the contemplated disclosure and, thus, the potential consequences of communication. This salience could lead to a disclosure to a smaller audience or within the confines of certain groups or privacy settings.

Some social technologies have already utilized this technique. For example, the professional social network site LinkedIn shows users who recently viewed their profile.[127] Shown in proximity to incipient but unpublished disclosures, these design features could serve to enhance obscurity-friendly practices such as encouraging users to be less explicit regarding personal information or to obfuscate the identity of the subject of the disclosure.

Designers could also combine our innate desire for conformity with feedback from the user's social graph to encourage obscurity friendly practices.[128] Although human beings might think they are uninfluenced by the behavior of their peers, empirical research demonstrates that people often simply conform to the behavior of others.[129] Thaler and

---

125. *Id.* (footnotes omitted).

126. *Id.* at 1044.

127. *Who's Viewed Your Profile?*, LINKEDIN, http://www.linkedin.com/static?key=pop/pop_more_wvmp (last visited Apr. 27, 2012).

128. *See* Hartzog & Stutzman, *Online Obscurity*, *supra* note 9.

129. *See, e.g.*, George A. Akerlof et al., *An Analysis of Out-of-Wedlock Childbearing in the*

Sunstein proposed that if many people within a particular community or "in group" are engaging in some kind of positive behavior (such as exercising), merely mentioning that fact to other members of the group might be able to produce significant changes in the other members' behavior.[130]

Given our tendency to look to other users of social technology for behavioral cues, designers could use statistics to encourage obscurity-friendly behavior. For example, designers could show users how many of their friends have utilized the privacy settings. Facebook already leverages the user's social graph by displaying how many mutual friends two "unconnected" users have.[131] Designers can implement these same kinds of cues to enhance obscurity at a low cost.

3. Content, Ordering, and Placement of Signals

Language and interactive features of websites often carry more weight than designers might intend. Organizations seeking to implement obscurity by design should be mindful that small changes in the prominence and number of instances of obscurity-related signals such as language emphasizing obscurity, privacy settings, options to hide from search engines and pseudonym policies, can have a significant effect on obscurity-friendly practices and user decisions.

Individuals often rely too much on a particular trait or piece of information when making decisions.[132] These overvalued pieces of information have been referred to as "anchors" because they become the starting points toward which decisions become biased.[133] Effective obscurity by design should optimize the placement of language and signals during the average user experience because they might become anchors for users and thus serve as behavioral interventions.

One form of this tactic has come to be known as a "just-in-time" alert and is supported as a valid "privacy by design" technique by the FTC.[134]

United States, 111 Q. J. ECON. 277 (1996); Bruce Sacerdote, *Peer Effects with Random Assignment: Results for Dartmouth Roommates*, 116 Q. J. ECON. 681 (2001).

130. *See* THALER & SUNSTEIN, *supra* note 115, at 60.

131. *See What Are Friendship Pages?*, FACEBOOK, https://www.facebook.com/help/220629401299124/ (last visited Apr. 19, 2013).

132. *See, e.g.*, Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124 (1974); *cf.* Gretchen B. Chapman & Eric J. Johnson, *The Limits of Anchoring*, 7 J. BEHAV. DECISION MAKING 223 (1994).

133. *See* Chapman & Johnson, *supra* note 132.

134. *See* FTC, MOBILE PRIVACY DISCLOSURES, *supra* note 11, at 15–16; *see also* Lauren Gelman, *FTC Recommends Best Practices for Mobile Privacy*, BLURRYEDGE STRATEGIES (Feb. 11, 2013), http://blurryedge.com/blurryedge-strategies/2013/02/ftc-recommends-best-practices-for-mobile-

According to the Commission, "[p]roviding such a disclosure at the point in time when it matters to consumers, just prior to the collection of such information by apps, will allow users to make informed choices about whether to allow the collection of such information."[135] The tech giant Apple has deployed just-in-time-disclosures in some aspects of its iOS6 operating system to obtain affirmative express consent for collection of personal information.[136]

With respect to just-in-time disclosures for social technologies, companies could introduce privacy settings early in the profile creation process and again at the point of disclosure. Designers could make the settings or language of privacy visible in the toolbar or the top of the homepage to increase awareness throughout the user experience. Companies could emphasize that pseudonyms are allowed before a profile name is chosen. These strategies could increase the likelihood that obscurity is a relevant anchor for users as they go about the process of selecting both content and audience.

Prominent and frequent obscurity-related signals could also combat people's tendency to assess risk using the most conveniently accessible example. This phenomenon has been labeled the "availability heuristic."[137] Reminding individuals of the obscurity in which their disclosures exist could help them properly gauge when to disclose further and when to curtail sharing.

Finally, prominent signals that remind users of the negative consequences of losing obscurity might help individuals be less forgetful of their potential audience. For example, users seeking to post a profanity-laden status update rife with personal information might be gently reminded that their co-workers, employer, or even their grandmother will be able to view the post. Users could then be given the option to tailor their update to a more discreet group.[138] Or designers could include very simple reminders at the point of disclosure explaining to users that their post will be available to anyone via search engines.

---

privacy.html.

135. FTC, MOBILE PRIVACY DISCLOSURES, *supra* note 11, at 15.

136. *See id.* at 16.

137. Tversky & Daniel, *supra* note 132, at 1127 ("There are situations in which people assess the frequency of a class or the probability of an event by the ease with which instances or occurrences can be brought to mind.").

138. Longtime users of word-processing software Microsoft Word might analogize such a guidance tool to "Clippy," the anthropomorphized paper-clip who asked if the Word users would like help when recognized user behavior associated with specific tasks. Of course, like Clippy, obscurity-reminders should also be easily disabled by the user.

4. Carefully Crafted Language

Finally, any effective implementation of obscurity by design should reflect an understanding of the power of framing to influence user decisions. The way that an issue like obscurity is framed by the designer's choice of language could have a significant effect on a user's disclosure decisions. Robert Entman stated, "To frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described."[139] In essence, "Frames highlight some bits of information about an item that is the subject of a communication, thereby elevating them in salience."[140]

One of the most widely cited examples of the power of framing involves an experiment by Daniel Kahneman and Amos Tversky. The experiment involved a significant number of participants who were each presented with statistically identical treatment options for a hypothetical disease. The treatment options, however, were framed differently to individual participants in terms of either likely deaths versus probable lives saved. The experiment showed that a significant number of participants' understanding of the problem, as well as their ultimate choice of treatment, changed depending on how the treatment option was framed.[141]

Obscurity can easily be framed as a positive or negative as well as a gain or a loss. Social technologies are designed for interaction and, as previously discussed, some might view obscurity as a hindrance to socialization. Thus, organizations seeking to implement obscurity by design could proactively address the conceptualization by framing obscurity as, we believe correctly, the natural state for most online socialization, as well as something to be "lost" if not protected.

When appropriate, framing obscurity as something the user already has and is subject to losing allows designers to leverage people's natural tendency to overvalue things they already have.[142] Thaler and Sunstein wrote, "People hate losses . . . . Roughly speaking, losing something

139. Robert M. Entman, *Framing: Toward Clarification of a Fractured Paradigm*, 43 J. COMM. 51, 52 (1993) (emphasis omitted).

140. *Id.* at 53.

141. *See* Daniel Kahneman & Amos Tversky, *Choices, Values, and Frames*, 39 AM. PSYCHOLOGIST 341 (1984).

142. *See, e.g.*, Daniel Kahneman, Jack Knetsh & Richard Thaler, *Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias*, 5 J. ECON. PERSP. 193 (1991).

makes you twice as miserable as gaining the same thing makes you happy."[143] This use of framing will aid users in maintaining the obscurity of their communications.

CONCLUSION

This Article has argued that while design-based solutions to protect privacy are promising, current proposals such as privacy by design have failed to tackle the social aspect of the Internet. This reluctance to tackle the "front end" of design-based solutions is understandable. The social web is messy, unpredictable, and amorphous. Mandating the inclusion of privacy practices into the design of social technologies can be problematic given that the goal of such technologies involves sharing personal information.

This Article has proposed a new design strategy for social technologies, which involves winnowing down from the unhelpful and vague conceptualization of privacy to the narrower, more accurate and attainable concept of obscurity. Information is obscure online if it exists in a context missing one or more key factors that are essential to discovery or comprehension. We have identified four of these factors as part of a non-exhaustive and flexible list: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity. The presence of these factors diminishes obscurity, and their absence enhances it. Those seeking to "bake" obscurity into the front-end of social technologies can do so through technologies, organizational policies, and behavioral interventions.

Where the pursuit of "privacy" in design often seems like a quest for near-perfect protection, the goal of designing for obscurity is that it be *good enough* for most contexts or to accommodate a user's specific needs**.** As the natural state for many online social communications, obscurity is the logical locus for the front end design of social technologies. Obscurity by design utilizes the full potential of design-based solutions to protect privacy and serve as a roadmap for organizations and regulators who seek to confront the vexing problems and contradictions inherent in social technologies.

143. THALER & SUNSTEIN, *supra* note 115, at 33.