4. A HEURISTICS APPROACH TO UNDERSTANDING PRIVACY-PROTECTING BEHAVIORS IN DIGITAL SOCIAL ENVIRONMENTS

ROBERT CAREY AND JACQUELYN BURKELL

I. INTRODUCTION

In this chapter, we consider ways that perceptions of harm and risk influence privacy-protecting behaviors in digital social environments (DSEs), with particular emphasis on Web logs and online social networks. By way of introduction, we would like to contrast two incidents from the world of online social networking that demonstrate how such perceptions may provoke very different responses to apparently similar privacy threats.

In 2006, Facebook introduced to its site a seemingly innocuous feature called an RSS news feed, which ensured that any changes a Facebook member made to his or her profile would be automatically disseminated to those members listed in his or her network. Since information of this sort was already evident to other Facebook users, the company supposed that the new feature was merely a convenient way to enhance information sharing among its members. Almost immediately, however, many Facebook users began to complain that the new feature was unacceptably invasive: "[T]he RSS feed publicizes potentially embarrassing developments including romantic breakups, friendships going sour, professional setbacks, and the like. Even though this information was available before, Facebook's active spreading of it via RSS feeds offended hundreds of thousands of the site's users."[1] Indeed, the feature became so unpopular among users that the company eventually capitulated and made the feature optional.

[1] Erik Sass, "Users Throw Book at Facebook," *Online Media Daily,* http://publications.mediapost.com/index.cfm?fuseaction=Articles.san&s=47811&Nid=23107&p=316563.

Almost exactly one year later, MySpace announced plans to collect and analyze the personal information members publish in their profiles. Fox Interactive intended to use these data to craft customized advertising specifically tailored to the individual enthusiasms and appetites of MySpace members. Unsurprisingly, privacy advocates argued that social network users should not be enrolled in a de facto surveillance campaign: "People should be able to congregate online with their friends without thinking that big brother, whether it is Rupert Murdoch or Mark Zuckerberg, are stealthily peering in," said Jeff Chester, Executive Director at the Center for Digital Democracy in Washington.[2] Interestingly, however, anecdotal reports suggested that users themselves were relatively phlegmatic about the matter. To our knowledge, there has been no concerted effort among MySpace users to stop the data collection.

These anecdotes suggest that DSE users are capable of remarkable ambivalence regarding their online privacy. Social networkers who believed that Facebook's news feed was publicizing intimate details about their personal lives were sufficiently angered to engage in a successful mass protest against the feature, yet MySpace's plans to scour its users' profiles for marketing purposes was greeted with comparative indifference. Considering that both situations involved exactly the same type of publicly-available personal information that users of the networks publish voluntarily, the contradictory behavior seems puzzling. We suggest, however, that the different responses can be explained by considering the way DSE users perceive various risks associated with their privacy, and the way such perceptions influence privacy-protecting behaviors. As the example above suggests, Facebook members had little trouble imagining likely harms if certain forms of personal information—changes to their occupational or relationship status, for example—were broadcast to all the people in their networks. From their perspectives, it mattered little whether the information was already evident on their profiles; the primary harm envisioned was embarrassment that the varied collection of people who constitute a Facebook network—including casual acquaintances who may not often visit their sites—would all be notified of consequential changes to one's life.

As several researchers have shown, DSE users often expend a great deal of effort to manage and protect certain aspects of their privacy, while remaining relatively unconcerned about other kinds of privacy threats. Accordingly, the purpose of this paper is to explore why users seem to be more highly attuned to certain kinds of risks associated with privacy in the context of DSEs. Our primary contention is that when people face complex or uncertain situations regarding privacy, they tend to rely on mental shortcuts to simplify their decision-making processes. We suggest that such shortcuts strongly influence both the way people

[2] Brad Stone, "MySpace Mining Members' Data to Tailor Ads Expressly for Them," *New York Times,* September 18, 2007, C1.

envision the risk of harms occurring to them as a consequence of their privacy being violated, and the consequent enacting of privacy-protecting behaviors. After reviewing relevant literature on the "privacy paradox" in online behavior—that is, the relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors[3]—we consider ways in which privacy is important to DSE users, and how these might be consequential for their understanding and assessment of privacy risks. Specifically, we examine heuristics, the mental shortcuts or "rules of thumb" that decision makers employ to make judgments under uncertainty. We review three heuristics—affect, representativeness, and availability—and speculate how each may contribute to risk judgments about privacy. Finally, we offer testable predictions regarding heuristic reasoning and privacy-related decision making in the context of DSEs.

II. THE PRIVACY PARADOX AND DIGITAL SOCIAL ENVIRONMENTS

Behavioral scientists have for some time been intrigued by the extent to which anticipatory self-reports—that is, statements of intention, attitude, or opinion—can be relied upon to predict behavior. After reviewing the relevant literature, O'Keefe, for example, noted that intention-behavior correlations were at best moderate, indicating that much of the time there is a fair or better-than-fair chance that people will behave in ways that belie their declared intentions.[4]

This disparity is so manifest in studies of privacy-protecting behaviors in online settings that Norberg, Horne, and Horne have called it the "privacy paradox."[5] As they put it, "for all the concern that people express about their personal information, which could be expected to drive one's intended and actual disclosure, our observations of actual marketplace behavior anecdotally suggest that people are less than selective and often cavalier in the protection of their own data profiles."[6] Although they were specifically referring to disclosure in the context of consumer marketing, researchers from various disciplines have made similar observations.[7] In short, although Internet users generally profess

[3] Patricia A. Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors" *Journal of Consumer Affairs* 41, no. 1 (2007): 100–126.

[4] Daniel J. O'Keefe, *Persuasion Theory and Research* (Thousand Oaks, CA: Sage Publications, 2002).

[5] Norberg, Horne, and Horne, "The Privacy Paradox," (n. 3).

[6] *Ibid.*, 101.

[7] See, for example, Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision Making," *Security and Privacy Magazine, IEEEE* 3, no. 1 (2005): 26–33; Joseph Turow, *Americans and Online Privacy: The System is Broken* (Philadelphia: Annenberg Public Policy Center, 2003); Mark S. Ackerman, Lorrie F. Cranor, and Joseph Reagle,

to be concerned about their privacy, they actually do little to protect it. One way in which this intention-behavior disjuncture is evident is the generally low level of knowledge about, and adoption of, privacy-protecting technologies in various online contexts.

A great deal of research suggests that many users exhibit functional illiteracy where privacy-protecting technologies are concerned. Milne, Bahl, and Rohm found that less than half the Internet users they studied set up their browsers to reject unnecessary cookies, cleared their computer memories after browsing, encrypted their e-mail, used anonymous re-mailers, or used anonymizers while browsing.[8] Jensen, Potts, and Jensen found most of their study subjects vastly overestimated their knowledge of privacy-related technologies and practices.[9] Slightly more than 90% of their study subjects, for example, claimed to understand Internet cookies, but only 14% could actually demonstrate such knowledge. Other investigators have found that users ignore or misunderstand privacy policies and privacy seals;[10] they are unaware of the amount and origin of spyware installed on their computers; and they do not realize that peer-to-peer file sharing programs—such as Kazaa—make sensitive data evident to others.[11] These and other studies support Turow's observation that "the overwhelming majority of U.S. adults who use the Internet at home have no clue about data flows . . . Even if they have a sense that sites track them and collect individual bits of their data, they simply don't fathom how those bits can be used."[12]

It is tempting to attribute the presumed privacy paradox to guilelessness about technology—in other words, to suggest that users who are deeply concerned about their online privacy are somehow stymied by their own ignorance of privacy-protecting technologies. Other studies, however, have shown that even in situations where technical expertise is irrelevant, people are easily induced

"Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences" (paper presented in the ACM Conference on Electronic Commerce, 1999), http://www.eecs.umich.edu/~ackerm/pub/99b28/ecommerce.final.pdf.

[8] George R. Milne, Andrew J. Rohm, and Shalini Bahl, "Consumers' Protection of Online Privacy and Identity," *The Journal of Consumer Affairs* 38, no. 2 (2004): 217–232.

[9] Carlos Jensen, Colin Potts, and Christian Jensen, "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior," *International Journal of Human-Computer Studies* 63, (2005): 203–227.

[10] Turow, *Americans and Online Privacy*; Anthony D. Miyazaki and Sandeep Krishnamurthy, "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *Journal of Consumer Affairs* 36, (2002): 28–49; Robert LaRose and Nora Rifon, "Your Privacy Is Assured—of Being Invaded: Websites with and without Privacy Seals," *New Media and Society* 8, no. 6 (2006): 1009–1029.

[11] Nathaniel S. Good and Aaron J. Krekelberg, "Usability and Privacy: A Study of Kazaa P2P File-Sharing," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI'03, 2003*, http://www.hpl.hp.com/techreports/2002/HPL-2002-163.pdf.

[12] Turow, *Americans and Online Privacy*, (n. 10).

to give up personal information.[13] As Norberg, Horne, and Horne suggest, "Perceptions of risk and trust are activated differently when intention measures are taken as compared to actual disclosure settings. . . . It appears that, in the realm of privacy, behavioral intentions may not be an accurate predictor of actual behavior."[14]

The importance of disclosure settings is illustrated in a study conducted by Berendt, Gunther, and Spiekermann, who investigated how privacy concerns relate to actual self-disclosing behavior.[15] They set up a laboratory experiment in which 206 participants took a virtual shopping trip in an online store. At the start of the trip, an anthropomorphic "bot" named Luci introduced herself. Luci's ostensible purpose was to provide product information and to guide participants through the virtual store; her actual purpose, however, was to ask questions of the shoppers. Researchers found that rates of disclosure, even to inappropriate questions, were "alarmingly high,"[16] concluding that "given the right circumstances, online users easily forget about their privacy concerns and communicate even the most personal details without any compelling reason to do so. This holds true in particular when the online exchange is entertaining and appropriate benefits are offered in return for information revelation."[17]

This observation has particular resonance for DSEs, which are almost entirely predicated on the beneficial consequences of personal disclosure. By its nature, social networking requires participants to reveal personal information—without at least some degree of disclosure, social networks cannot be cultivated or maintained.[18] Similarly, most blogs (short for Web logs) fall into the category of personal journals, whose chief purpose is to reflect the thoughts, feelings, and everyday details of their authors' lives.[19]

[13] See, for example, Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox," (n. 3); Acquisti and Grossklags, "Privacy and Rationality," (n. 7).

[14] Norberg, Daniel R. Horne, and David A. Horne, "The Privacy Paradox," (n. 3).

[15] Bettina Berendt, Oliver Günther, and Sarah Spiekermann, "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior,*" Communications of the ACM* 48, no. 4 (2005): 101–106.

[16] Berendt, Günther, and Spiekermann, "Privacy in E-Commerce," (n. 15), 104.

[17] *Ibid.*, 103.

[18] Judith Donath and Danah Boyd, "Public Displays of Connection," *BT Technology Journal* 22, no. 4 (2004): 71–82; Roya Feizy, "An Evaluation of Identity on Online Social Networking: MySpace," in *Eighteenth International ACM Conference on Hypertext and Hypermedia, Manchester, Sept 2007,* http://www.informatics.sussex.ac.uk/research/groups/softsys/papers/feizy-hypertext07.pdf 2007.

[19] Susan Herring, Lois Ann Scheidt, Sabrina Bonus, Elijah Wright, "Bridging the Gap: A Genre Analysis of Weblogs," in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04),* http://www.ics.uci.edu/~jpd/classes/ ics234cw04/herring.pdf; Fernanda, B. Viégas, "Bloggers' Expectations of Privacy and Accountability: An Initial Survey," *Journal of Computer-Mediated Communication 10, no.* 3 (2005): article 12; Bonnie Nardi, Diane Schiano, Michelle Gumbrecht, and Luke Schwarz, "Why We Blog," *Communications of the ACM* 47, no. 12 (2004a): 41–46.

Given the centrality of self-revelation to DSE productions, it is not surprising that they constitute rich troves of personal information. Many profiles on social networking sites, for example, have been shown to include identifying information such as full or partial name, sex, birth date, phone number, high school, or current residence.[20] Some research has verified that much of the personal information culled from samples of network profiles is indeed accurate.[21] Many bloggers, too, provide full or partial names, contact information, and demographic information such as age, address, or occupation.[22] Personal photographs are another common feature of blogs and social network profiles; indeed, the majority of MySpace and Facebook profiles include an image,[23] and many of these are photographs suitable for direct identification.[24]

The revelation of such detailed personal information through blogs and social network profiles obviously invites a range of privacy threats. Marketers, for example, are interested in non-identifying personal information reflecting attitudes, beliefs, desires, and preferences, to support research agendas,[25] identify market

[20] Amanda Lenhart and Mary Madden, *Teens, Privacy, & Online Social Networks* (Washington, DC: PEW Internet and American Life Project, 2007); Ralph Gross and Alessandro Acquisti, "Information Revelation and Privacy in Online Social Networks (the Facebook Case)," in *ACM Workshop on Privacy in the Electronic Society (WPES), 2005*, http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf; Cliff Lampe, Nicole Ellison, and Charles Steinfield, "A Face(book) in the Crowd: Social Searching vs. Social Browsing," in *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work,* http://delivery.acm.org/10.1145/1190000/1180901/p167-lampe.pdf?key1=1180901&key2=0211721911&coll=GUIDE&dl=GUIDE&CFID=37188441&CFTOKEN=27270162; Harvey Jones and José Hiram Soltren, "Facebook: Threats to Privacy," *Massachusetts Institute of Technology*, http://www-swiss.ai.mit.edu/6805/student-papers/fall05-papers/facebook.pdf.

[21] Alessandro Acquisti and Ralph Gross, "Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook" (paper presented at PET 2006), http://privacy.cs.cmu.edu/dataprivacy/projects/ facebook/facebook2.pdf.

[22] Herring et al., "Bridging the Gap"; David A. Huffaker and Sandra L. Calvert, "Gender, Identity, and Language Use in Teenage Blogs," Journal of Computer-Mediated Communication *10, no.* 2, article 1 (2005), http://jcmc.indiana.edu/vol10/issue2/huffaker.html; Bonnie A. Nardi, Diane J. Schiano, and Michelle Gumbrecht, "Blogging as Social Activity, or, Would You Let 900 Million People Read Your Diary?" in *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work, CSCW'04*, http://home.comcast.net/~diane.schiano/CSCW04.Blog.pdf; Viégas, "Bloggers' Expectations," (n. 19).

[23] Catherine Dwyer, Starr Roxanne Hiltz, and Katia Passerini, "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace," in *Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado August 09-12 2007*, http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf; Lenhart and Madden, *Teens, Privacy, & Online Social Networks*, (n. 20).

[24] Gross and Acquisti, "Information Revelation and Privacy," (n. 20).

[25] Mike Thelwall, "Blog Searching: The First General-Purpose Source of Retrospective Public Opinion in the Social Sciences?" *Online Information Review* 31, no. 3 (2007): 277–289.

trends,[26] select potential customers who are likely to influence others,[27] or target ads to specific consumers who are likely to respond based on their profile information.[28] Traditional concerns about online identity theft, fraud, and stalking have been exacerbated by the inclusion of personal photographs in various DSE applications, compromising visual anonymity,[29] and new applications allow for sophisticated data mining of blogs and social network profiles.[30] Additionally, archiving renders even deleted data accessible for analysis for an extended period.

Despite these threats, the privacy paradox appears to be just as operative in the DSE context as it is in more traditional online settings. A survey of Facebook users, for example, found a strong discrepancy between subjects' stated privacy attitudes and their actual privacy-protecting behaviors.[31] The researchers "detected little or no relation between participants' reported privacy attitudes and their likelihood of providing [personal] information" online. Even among the students who claimed to be very concerned about privacy, 40% provided their class schedule on Facebook, 22% published their address, and 16% posted both. Along similar lines, a 2006 survey suggests that some DSE users may have difficulty envisioning possible harms arising from publishing personal information online. The survey found that "40% of employers say they would consider the Facebook profile of a potential employee as part of their hiring decision, and several reported rescinding offers after checking out Facebook."[32] And yet, when students were informed of this, 42% thought it was a violation of privacy for employers to investigate their profiles, and "64% of students said employers should not consider Facebook profiles during the hiring process."[33]

[26] Qiaozhu Mei, Chao Liu, Hang Su, and ChangXiang Zhai, "A Probabilistic Approach to Spatiotemporal Theme Pattern Mining on Weblogs," in *Proceedings of the 15th international Conference on World Wide Web (WWW 2006)*, http://sifaka.cs.uiuc.edu/czhai/pub/www06-blog.pdf; Gilad Mishne and Maarten de Rijke, "Capturing Global Mood Levels Using Blog Posts," *American Association for Artificial Intelligence 2006 (www.aaai.org)*, http://staff.science.uva.nl/~gilad/pubs/aaai06-blogmoods.pdf.

[27] Pedro Domingos and Matt Richardson, "Mining the Network Value of Customers," in *Proceedings on the Seventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2001*, http://www.cs.washington.edu/homes/pedrod/papers/kdd01a.pdf. 2001.

[28] Hugo Liu and Patti Maes, "Interestmap: Harvesting Social Network Profiles for Recommendations," in *Workshop: Beyond Personalization 2005, IUI'05*, http://ambient.media.mit.edu/ assets/_pubs/BP2005-hugo-interestmap.pdf 2005.

[29] Hua Qian and Craig R. Scott, "Anonymity and Self-Disclosure on Weblogs," *Journal of Compuer-Mediated Communication* 12, no. 4 (2007): 1428–1451.

[30] Gross and Acquisti, "Information Revelation and Privacy," (n. 20).

[31] Acquisti and Gross, "Imagined Communities," (n. 21).

[32] University of Dayton, "Facing the Consequences of Facebook," *UD News*, http://universityofdayton.blogs.com/local/2006/11/facing_the_cons.html.

[33] *Ibid.*

III. A STUDIED MINUET: PRIVACY BEHAVIORS IN DSES

Some researchers have, intriguingly, painted a more complex portrait of privacy-protecting behaviors in DSE environments than the foregoing suggests. Nardi et al. described blogging as a "studied minuet" between author and reader—many bloggers are aware that at least a portion of their audience consists of people with whom they have some offline connection.[34] Since bloggers are concerned that their writings could impinge on these relations, they expend a great deal of effort tailoring their entries to accommodate the sensitivities of their readers.[35] One survey found that bloggers were most sensitive to privacy implications when blogging about friends and family.[36] The same survey results also indicated that 62% of respondents had considered that some topics were "too personal" to write about. Indeed, several respondents explained "that they had encountered trouble with acquaintances in the past because they had disclosed their names on blog entries. After having gotten in trouble, respondents became more sensitive to the issue of identification."[37] The primary response to such concerns is to modify content or to limit the blog audience by using filters.[38]

Participants in social networking sites demonstrate similar concerns, insofar as their productions are also directed toward an audience of family, friends, and acquaintances. In one study of Facebook, for example, more than half the subjects identified friends, acquaintances, classmates, fellow students, and family as their target audience, while fewer than half intended their profiles to be viewed by strangers, professors, administrators, or those in law enforcement.[39] In unpublished interviews we conducted with users of online social networks, we found that most participants were primarily attuned to privacy concerns arising from their immediate social relations, rather than unknown others. The following comment is illustrative:

> I'm not really concerned what random third parties think. I mean, it doesn't affect my life. They're never going to affect my life. It's those middle people, like the ex-boyfriends and the friends who you are not friends with anymore. Then it would affect your life because they're out to get you.

[34] Nardi, Schiano, and Gumbrecht, "Blogging as Social Activity," (n. 22).

[35] Qian and Scott, "Anonymity and Self-Disclosure on Weblogs," (n. 29).

[36] Viégas, "Bloggers' Expectations of Privacy and Accountability," (n. 19).

[37] *Ibid.*

[38] Qian and Scott, "Anonymity and Self-Disclosure on Weblogs," (n. 29); Nardi, Schiano, and Gumbrecht, "Blogging as Social Activity," (n. 22).

[39] Nicole B. Ellison, Charles Steinfield, and Cliff Lampe, "The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites," *Journal of Computer-Mediated Communication* 12, (2007): 1143–1168.

Like bloggers, social network users have developed a repertoire of informal privacy-protecting tactics intended to avoid causing embarrassment to themselves, friends, or family, and foremost among these is content modification.[40]

It appears, then, that DSE users exhibit ambivalence where privacy-protecting behaviors are concerned. As the foregoing research suggests, even those who profess to be concerned about their privacy publish a great deal of revealing personal information about themselves. Users appear to be unaware or unmindful of possible harms arising from profligate disclosures, particularly harms visited upon them by unknown others. Indeed, when users are moved to enact privacy-protecting behaviors, these efforts consist primarily of modifying the stylistics or content of their communications so as to be less revealing to known others. In general, bloggers and social network participants seem most sharply attentive to the constellation of concerns surrounding what DeCew has called expressive privacy,[41] which Goldie summarizes as "one's ability to freely choose, act, self-express and socially interact."[42] For Goldie, the protection of expressive privacy—an actor's efforts to control the degree to which he or she is known by preferred others—is central to the development of close relationships: "Because intimacy is based on the self-disclosure of information, if we were unable to choose or control what information we give out or the degree to which we allow other people to know us, intimate relationships would cease to exist, and essentially everyone would know everything about everyone."[43]

As several researchers have suggested, however, users who are attuned solely to violations of their expressive privacy remain at risk for other sorts of privacy-related harms. Gross and Acquisti point out that the fragile privacy protection afforded to social network users can be circumvented through social engineering or search techniques, such that "one may conclude that the personal information users are revealing even on sites with access control and managed search capabilities effectively becomes public data."[44] Thus, we return to the central question that animates this chapter: why do many users appear to be attuned to certain harms associated with privacy in the context of DSEs, but not to other types of harms? In the remainder of this chapter, we examine the cognitive techniques that decision makers commonly employ to make judgments about risks, and we speculate about ways these may be consequential for DSE users.

[40] Lenhart and Madden, *Teens, Privacy, & Online Social Networks*, (n. 20).

[41] Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics & the Rise of Technology* (Ithaca: Cornell University Press, 1977).

[42] Janis L. Goldie, "Virtual Communities and the Social Dimension of Privacy," *University of Ottawa Technology and Law Journal* 3, no. 1 (2006): 139.

[43] *Ibid.*, 140.

[44] Gross and Acquisti, "Information Revelation and Privacy," (n. 20).

IV. HEURISTICS, BIASES, AND THE ESTIMATION OF RISK

Decisions about whether to make personal information evident to others require some sort of calculation regarding the relative costs and benefits of disclosure. In the context of DSEs, this imperative is complicated by the uncertain nature of many harms. For example, while it is certainly possible that a potential employer might view one's compromising Facebook photographs, this outcome is far from certain. In weighing the costs of disclosure, therefore, it is not enough to imagine what might happen—the harm—since this may or may not actually transpire. The decision maker must also come to some reckoning of the harm's likelihood—in other words, the risk.

The central problem of risk assessment, however, is that risks are often unknown. From the decision maker's limited perspective, there may be no way to find out how frequently certain harms occur. In many situations, therefore, it seems there is no reliable way for users to evaluate their own risk of negative outcomes. Kahneman and Tversky called this situation "judgment under uncertainty" and suggested that, when faced with the task of assessing the unknown likelihood of an uncertain event, decision makers are forced to rely on heuristics to make their judgments.[45] These cognitive shortcuts are designed to assist decision makers when information, along with other cognitive resources such as time and attention, is limited.[46]

Heuristics are helpful for risk assessment insofar as they allow the decision maker to bypass complex calculations regarding probability. Often, the result of heuristic reasoning is a response that "satisfices,"[47] meeting the decision maker's immediate need without necessarily being the optimal or exact response. In some cases, the use of heuristics to make decisions has been shown to produce better results than those generated by a fully rational approach.[48] Heuristics may also lead to biases, in which case the decision maker's best guess results in estimates that are predictably biased. In the following section, we consider ways in which three heuristics—affect, availability, and representativeness—might influence DSE users' apprehension of privacy-related risks.

A. The Affect Heuristic

As we have suggested, conventional approaches to the study of risk management have often configured actors as rational decision makers capable of applying

[45] Daniel Kahneman and Amos Tversky, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, (1974): 1124–1131.

[46] Herbert Simon, "Rational Choice and the Structure of the Environment," *Psychological Review* 63, (1956): 129–138.

[47] *Ibid.*

[48] Gerd Gigerenzer and Daniel G. Goldstein, "Reasoning the Fast and Frugal Way: Models of Bounded Rationality," *Psychological Review* 103, no. 4 (1996): 650–669.

logic to situations requiring self-protection. Protection motivation theory (PMT), for example, suggests that actors invoke protective behaviors after having appraised the advantages and disadvantages of responding to a perceived threat. This and cognate approaches—such as the theory of reasoned action (TRA) and subjective expected utility (SEU) theory—share "a cost-benefit analysis component in which the individual weighs the costs of taking the precautionary action against the expected benefits of taking that action."[49] These theories assume that the actor possesses sufficient ability to calculate the probabilities of harms or rewards arising from any action.

Increasingly, however, the notion of bounded rationality[50] has become consequential for studies of risk perception. The concept of bounded rationality is consonant with a growing belief among researchers that most risk analysis is performed expediently by what Slovic et al. have called the "experiential" mode of thinking, which is "intuitive, fast, mostly automatic, and not very accessible to conscious awareness."[51] Heuristic processing is central to the experiential system in that it operates quickly and intuitively to make crucial information salient to the decision maker.[52]

One such type of processing is the affect heuristic. "Affect" refers to a feeling of goodness or badness arising from perceptions of a positive or negative stimulus. Researchers argue that such feelings are crucial for the apprehension of risk: if a person's feelings toward an activity are favorable, they are inclined to judge the risks as low and the benefits as high; if their feelings are unfavorable, they tend to judge the opposite—high risk and low benefit.[53] In this sense, affect precedes and directs the individual's judgment of risk and benefit. Finucane et al. examined this hypothesis by presenting decision makers with information designed to influence affect without directly influencing perception of risks or benefits.[54] The researchers demonstrated that when study subjects were given information indicating that nuclear power was highly beneficial—for example,

[49] Donna L. Floyd, Steven Prentice-Dunn, Ronald W. Rogers, "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Social Psychology* 30, no. 2 (2000): 408.

[50] Simon, "Rational Choice and the Structure of the Environment," (n.46).

[51] Paul Slovic, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor, "Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality," *Risk Analysis* 24, no. 2 (2004): 311.

[52] Ellen Peters, Kevin D. McCaul, Michael Stefanek, and Wendy Nelson, "A Heuristics Approach to Understanding Cancer Risk Perception: Contributions from Judgment and Decision-Making Research," *Annals of Behavioral Medicine* 31, no. 1 (2006): 45–52.

[53] Slovic, Finucane, Peters, and MacGregor, "Risk as Analysis and Risk as Feelings," 311–322 (n. 51).

[54] Melissa L. Finucane, Ali Alhakami, Paul Slovic, and Stephen M. Johnson, "The Affect Heuristic in Judgments of Risks and Benefits," *Journal of Behavioral Decision Making* 13, no. 1 (2000): 1–17.

that it does not depend on fossil fuel—they judged its overall risk to be low. Conversely, when subjects were given information suggesting that nuclear power was of minimal benefit—that it produces only a small percentage of the nation's electricity—they judged the risk from nuclear power to be high. Thus, the experiment supports the theory that risk and benefit judgments are influenced, at least in part, by affective evaluation.

We suggest that the affective and experiential nature of risk perception may be relevant to decision making regarding privacy in digital social environments insofar as there is abundant evidence that the kind of revelatory self-writing these media entail effect a positive affect—in other words, that writing about oneself to a real or imagined audience makes one feel good. Much research indicates that writing about life events reduces both negative mood and stress symptoms,[55] by reducing negative mood after traumatic events,[56] and decreasing symptoms of worry, anxiety disorder, and depression.[57] Some research suggests that the expressive self-writing implicit in blogging and social networking affords the same benefits. Finding that many of the bloggers they studied wished to "work through" difficult, traumatic, or personal matters, Nardi et al. state, "[t]he format of frequent post, diary-style, is both outlet and stimulus for working through issues. Often, bloggers turned to the blog as a welcome relief valve, a place to 'get closure out of writing.'"[58]

The affective nature of blogging and social networking may explain why users are sometimes unmindful of certain kinds of privacy risks when they write about themselves. Bloggers and participants in social networking sites are aware of privacy threats, and yet they continue to provide extensive personal information.[59] Research has shown that attention to salient affective cues can

[55] E.g., Stephen J. Lepore, Melanie A. Greenberg, Michelle Bruno, and Joshua M. Smyth, "Expressive Writing and Health: Self-Regulation of Emotion Related Experience, Physiology, and Behaviour," in *The Writing Cure: How Expressive Writing Promotes Health and Emotional Well-Being*, ed. S. J. Lepore & J. M. Smyth (Washington, DC: American Psychological Association, 2002), 99–117; James W. Pennebaker, "The Effects of Traumatic Disclosure on Physical and Mental Health: The Values of Writing and Talking about Upsetting Events," *International Journal of Emergency Mental Health* 1, (1999): 9–18; Denise M. Sloan and Brian P. Marx, "Taking Pen to Hand: Evaluating Theories Underlying the Written Disclosure Paradigm," *Clinical Psychology: Science and Practice* 11, (2004): 121–137; Joshua M. Smyth, "Written Emotional Expression: Effect Sizes, Outcome Types, and Moderating Variables," *Journal of Consulting and Clinical Psychology* 66, (1998): 174–184.

[56] Laura A. King, "The Health Benefits of Writing about Life Goals," *Personality and Social Psychology Bulletin* 27, (2001): 798–807.

[57] Natalie Goldman, Michael J. Dugas, Kathryn A. Sexton, and Nicole J. Gervais, "The Impact of Written Exposure on Worry: A Preliminary Investigation," *Behavior Modification* 31, no. 4 (2007): 512–538.

[58] Nardi et al., "Why We Blog," 8 (n. 19).

[59] Gross and Acquisti, "Information Revelation and Privacy," (n. 20).

lead to a neglect of the probabilistic information necessary to estimate risk accurately.[60] Along similar lines, DSE users whose activities provide them with strong positive feelings may underestimate the harms arising from the disclosure of personal information.

B. The Availability Heuristic

The availability heuristic makes it possible for decision makers to gauge the likelihood of an outcome by retrieving relevant examples from their memories. Outcomes are judged probable if instances of analogous phenomena can be readily brought to mind. This cognitive shortcut allows the decision maker to estimate probabilities expediently by avoiding time-consuming calculations. In one experiment, subjects were asked to estimate which occurs more frequently in the English language: words beginning with the letter "k," or those in which the letter "k" appears in the third position. Specific instances of the first category easily come to mind, while recalling words that fit the second category is an effortful process.[61] The common conclusion, therefore, is that there are more words that start with "k." In fact, the opposite is true.

Several factors influence the application of this heuristic. One of these is retrievability. As we have noted, categories of events or objects that are easy to recall are judged to be more probable. Consequently, events that are more recent, salient, or familiar to the decision maker tend to be judged more likely because they are easily retrievable. There are numerous situations, however, in which decision makers are required to judge the probability of events for which they can recall no specific instances. In these situations, decision makers judge an event to be more likely if it is easier to imagine or construct.

One consequence of the availability heuristic is that the perception of risk increases with direct experience of negative outcomes. In other words, if a person's experience of a negative outcome is memorable, he or she will be more attuned to risk in comparable subsequent situations because examples of negative outcomes are readily available to him or her. Researchers have shown, for example, that there exists a tendency to overestimate cancer risk among people who have friends or acquaintances (not relatives with whom they might share a genetic risk) with cancer.[62] Along similar lines, direct experience with natural disasters has been shown to increase the perception of risk for similar disasters,[63]

[60] Yuval Rottenstreich and Christopher K. Hsee, "Money, Kisses, and Electric Shocks: On the Affective Psychology of Risk," *Psychological Science* 12, (2001): 185–190.

[61] Amos Tversky and Daniel Kahneman, "Availability: A Heuristic for Judging Frequency and Probability," *Cognitive Psychology* 5 (1973): 207.

[62] K. Fiandt, C.H. Pullen, and S.N. Walker, "Actual and Perceived Risk for Chronic Illness in Rural Older Women," *Clinical Excellence for Nurse Practitioners* 3 (1999): 105–115.

[63] Michael Siegrist and Heinz Gutscher, "Flooding Risks: A Comparison of Lay People's Perceptions and Experts' Assessments in Switzerland," R*isk Analysis* 26, (2006): 971–979.

while products are viewed as more likely to fail in the future if past failures have been memorable.[64]

The availability heuristic may account for the fact that DSE users often expend a great deal of effort to manage elements of their expressive privacy while remaining indifferent to other kinds of privacy violations. Bloggers and social networkers demonstrate ambivalent behavior in this respect. Although they express concern about socially distant individuals accessing their personal information, much of their actual privacy-protecting behavior tends to be organized around more intimate relations.[65] The mass protest against Facebook's news feed and MySpace users' relative indifference to the data mining of their profiles are illustrative. We suggest that one reason DSE users appear to be more attuned to violations of expressive privacy is the result of the associated harms that are more readily available to them; in other words, it is easier for them to recall uncomfortable consequences of the release of "destructive information" simply because these sorts of episodes are commonplace.[66] Conversely, data mining may excite little interest from DSE users because the harms resulting from this activity are not readily available.

The media are also a source of information about privacy risks, which may be consequential for risk assessments regarding privacy. Since availability may be influenced by emotionally compelling and vivid information,[67] highly publicized events are likely to be more salient and, therefore, more readily remembered. An example is the publicity surrounding "To Catch a Predator," a 2004 series on the NBC news magazine program *Dateline*. The series included three programs in which hidden cameras captured men meeting teenagers, who turned out to be volunteers with a group dedicated to policing Internet stalking. Anecdotal reports describe the series as a "tipping point" that sparked a wave of concern about social networking sites that some experts described as overreaction:

> "Everyone is freaked," said Parry Aftab, the director of Wired Safety, a non-profit group of volunteers who conduct safety meetings for parents. "They are convinced the Internet Bogeyman is going to come into their window," she said. "To date that has not happened."[68]

Indeed, the *New York Times* story quoted above noted that the U.S. Department of Justice's Internet Crimes Against Children task forces made 600 arrests in 2005, but few of these were for actual assaults. It would seem that if the *Dateline*

[64] Valerie S. Folkes, "The Availability Heuristic and Perceived Risk," *Journal of Consumer Research* 15, no. 1 (1988): 13–23.

[65] Janis L. Goldie, "Virtual Communities and the Social Dimension of Privacy," *University of Ottawa Technology and Law Journal* 3, no. 1 (2006): 135–166.

[66] Erving Goffman, *The Presentation of Self in Everyday Life* (New York: Doubleday, 1959), 144.

[67] Peters, McCaul, Stefanek, and Nelson, "A Heuristics Approach," (n. 52).

[68] A. Bahney, "Don't Talk to Invisible Strangers," *New York Times*, March 9, 2006, G1.

series did heighten parental concern about social networking sites, it did so by providing parents with highly imaginable examples of negative outcomes. Interestingly, some research suggests that although media representations can influence availability, they do so only in the absence of personal experience.[69] This may account for the fact that social networkers may underestimate potential privacy threats. Indeed, a 14-year-old social networker interviewed by the *New York Times* noted, "[p]arents are going to panic. They are going to overreact. Suddenly somebody, some random person in Illinois or somewhere, gets kidnapped, and then it's a problem."[70] This user's personal experience of social networking may provide him with a different basis with which to calculate the probability of negative outcomes.

C. The Representativeness Heuristic

The representativeness heuristic allows a decision maker to estimate probability by relying on mental models or stereotypes, thereby circumventing more complex calculations. It is sometimes used to estimate likelihoods associated with group or category membership. If, for example, a decision maker wanted to know how likely it is that object A is a member of category X, he or she might first recall specific traits he or she believes to be characteristic of typical category X members. If object A also possesses these traits, then, in the decision maker's estimation, it is likely to be a member of category X.

The representativeness heuristic was first articulated by Kahneman and Tversky, who devised an experiment in which subjects were required to determine whether an individual was more likely to be a lawyer or an engineer.[71] Subjects were told that the target individual was drawn from a larger group of whom 70% were lawyers and 30% were engineers. Subjects were also given a list of traits possessed by the target individual (these traits were carefully chosen to represent stereotypes associated with either lawyers or engineers). Rather than considering the actual base rate of the two occupations in the group from which the target individual was drawn, subjects tended to rely instead on the stereotypical traits to make their judgments. Thus, if the description of the target individual fit the stereotype of a lawyer, he was judged more likely to be a lawyer; if his description fit the stereotype of an engineer, he was judged more likely to be an engineer.

The representativeness heuristic has been shown to have wide application in everyday risk assessments. For example, the logic of the heuristic may explain why certain individuals underestimate their risk of disease if they feel that they

[69] Rick W. Busselle and L.J. Shrum, "Media Exposure and Exemplar Accessibility," *Media Psychology* 5, no. 3 (2003): 255–282.

[70] Bahney, "Don't Talk to Invisible Strangers," G1 (n. 68).

[71] Kahneman and Tversky, "Judgment under Uncertainty," (n. 45).

do not resemble someone with the disease.[72] As Kahneman and Tversky's experiment demonstrates, over-reliance on stereotypes often causes people to ignore other information when making risk judgments.[73] Researchers have speculated that because heart disease is more stereotypic of men, women incorrectly view their risk of breast cancer as greater than the risk of heart disease.[74]

In the realm of privacy, this heuristic may operate when DSE users underplay the possibility that they may be vulnerable to harms because they do not identify themselves with someone who is stereotypically at risk. A 23-year-old social networker, in an unpublished interview we conducted, claimed not to be concerned about stalkers, even though she acknowledged that she had divulged a great deal of personal information in her profile: "I don't know. I think that's kind of an early, twelve-year-old kind of fear, that stalkers are looking for you on the Internet. And I don't think it's anything other than just creepy people that are looking to find information about you." According to this user's schema, she does not belong to the category of users at risk for stalking, and, therefore, she concludes that her probability of experiencing this threat is low.

It is also possible that the way users conceptualize privacy threats makes it easier for them to invoke the representativeness heuristic. Experts and non-experts differ in the mental models they use to conceptualize computer security risks.[75] Another DSE user we interviewed claimed, "I guess I'm not really adventurous, I just go into the same sites I'm familiar with, for the most part. I do think Internet activity should be private, other than if it's being used for criminal intent or anything like that. But I'm not doing that." This user equated threats to privacy with the surveillance of Internet traffic for criminal justice purposes; since she was not engaged in criminal activity, she believed she was not at risk for privacy violation.

V. CONCLUSION

We began this paper by reviewing the privacy paradox and its relevance to DSEs. We also suggested that the paradox takes on a more complex character in these environments. Users of DSE applications claim privacy concerns, yet continue to reveal personal information. At the same time, they demonstrate different responses to two types of privacy concerns: they are more likely to enact behaviors

[72] Mark Parascandola, Jennifer Hawkins, and Marion Danis, "Patient Autonomy and the Challenge of Clinical Uncertainty," *Kennedy Institute of Ethics Journal* 12 (2001): 245–264.

[73] Kahneman and Tversky, "Judgment under Uncertainty," (n. 45).

[74] Peters, McCaul, Stefanek, and Nelson, "A Heuristics Approach," 47 (n. 52).

[75] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp, "Mental Models of Computer Security Risks," in *The Sixth Workshop on the Economics of Information Security–WEIS, 2007*, http://weis2007.econinfosec.org/papers/80.pdf.

to protect privacy in their personal relationships, and less likely to act to protect their privacy in relation to unknown others. Following Goldie and DeCew, we have used the term expressive privacy to refer to the former.[76]

Under models of protective behavior or market exchange, decisions about the release of personal information involve a weighing of the risks and benefits associated with such release. In DSEs, the risks are uncertain. In fact, it is difficult to specify the precise chance that negative privacy outcomes will occur. Faced with the estimation of uncertain risks, decision makers are forced to rely on cognitive heuristics—shortcuts that allow them to establish some reasonable estimate of risk in the absence of specific information about actual risk levels.[77] We suggest that the application of these heuristics in the estimation of privacy risks in DSEs could account for both aspects of the privacy paradox observed in these environments.

The analysis presented in this chapter is largely speculative, and four specific predictions emerge that invite empirical investigation. Research on these questions will help to identify whether perceived risk, and the heuristics involved in that assessment, can account for the privacy paradox evident in DSEs.

Prediction 1: Participants in DSEs will be most attuned to expressive privacy risks. Our speculations rest on the initial assumption that DSE participants have different perceptions of risks associated with various privacy hazards. In particular, we predict higher perception of risks associated with expressive privacy, compared to other privacy hazards. One way to assess these risk perceptions is to have participants generate lists of privacy concerns, rating their perceived risk of experiencing each negative outcome. This approach avoids cuing respondents to specific privacy issues, and instead focuses on those that are salient. We would make two specific predictions in this work: first, that the list of concerns generated would be primarily related to expressive privacy; and second, that among those concerns identified, expressive privacy concerns will receive higher ratings of perceived risk.

Prediction 2: To the extent that DSE participants enjoy their online experience, they will have decreased overall privacy risk perceptions. According to our analysis, the use of the affect heuristic should lead to reduced privacy concerns in DSEs. Two approaches can be used to investigate this prediction: a descriptive approach, and an experimental approach. If affect influences perceived privacy risk, then users of DSEs who feel positive about their participation should also perceive lower risk of privacy breaches. If this association is observed among DSE users, then an experiment could determine whether different risk evaluations can be produced by affect manipulations. Specifically, we would predict that users who are

[76] Goldie, "Virtual Communities," (n. 42); DeCew, *In Pursuit of Privacy*, (n. 41).

[77] Kahneman and Tversky, "Judgment under Uncertainty," (n. 45).

induced to have positive affect regarding their DSE use through informational or other interventions will show decreased perceptions of privacy risks.

Prediction 3: To the degree that DSE participants can easily recall specific instances of privacy violations, they will have an increased perceived risk of that type of privacy violation. If the availability heuristic is responsible for different perceptions of expressive and non-expressive privacy risks in DSEs, then instances of expressive privacy breaches should be more available to users of these applications. Asked to recall or generate instances of negative consequences of privacy breaches, they should offer more examples of expressive privacy breaches, claim more direct knowledge of those breaches (e.g., personal experience rather than media reports), and offer a more detailed report of such breaches. Furthermore, measures of the accessibility of such instances (e.g., number recalled, reported ease of recall, amount of detail provided) should be positively associated with perceived risk of expressive privacy breaches. The same association is expected to hold for breaches of non-expressive privacy, although the overall availability of such outcomes is predicted to be lower.

Prediction 4: To the extent that DSE participants view themselves as different from those likely to experience privacy violations, they will evaluate their risk as lower. We suggest that the representativeness heuristic could explain depressed risk perceptions associated with non-expressive breaches, precisely because DSE participants view themselves as different from those at risk. If true, DSE participants should associate different qualities with individuals at higher risk for expressive versus other types of privacy breaches. Moreover, they should see themselves as more similar to the profile of those at risk for expressive privacy breaches. Finally, perceived risk of breaches of non-expressive privacy should be positively related to the perceived similarity between oneself and the "at-risk" group.