

## Chapter 3

# **SOCIAL NORMS, SELF CONTROL, AND PRIVACY IN THE ONLINE WORLD**

Katherine J. Strandburg

*Assistant Professor of Law, DePaul University College of Law. An extended version of this chapter will be published as *Privacy, Rationality, Temptation, and the Implications of Willpower Norms* (forthcoming Rutgers Law Review, 2005).*

**Abstract:** This chapter explores ways in which human limitations of rationality and susceptibility to temptation might affect the flow of personal information in the online environment. It relies on the concept of “willpower norms” to understand how the online environment might undermine the effectiveness of social norms that may have developed to regulate the flow of personal information in the offline world. Finally, the chapter discusses whether legal regulation of information privacy is an appropriate response to this issue and how such regulation should be formulated in light of tensions between concerns about self-control and paternalism.

**Key words:** willpower, temptation, self control, data mining, online communities, privacy torts, social norms

## **1. INTRODUCTION**

Everyone over the age of four or five knows that certain personal information is appropriately discussed in some social contexts, but not in others. Teenagers have an acronym for inappropriate personal disclosures; “TMI,” they say, “Too much information!” Social norms delineate the types of personal information that are appropriately disclosed in particular circumstances and those who do not follow these personal information norms are looked upon with disfavor. This reluctance to receive certain personal information is surprising in light of the important role that accurate information plays in making decisions and assessing options, in

interpersonal as well as commercial contexts. In a more extended version of this chapter,<sup>1</sup> I argue that the complicated and nuanced social norms that surround the flow of personal information are examples of “willpower norms” which can arise in response to the interplay between self-control temptation and human cognitive limitations.

Here I focus on the implications of the analysis of social norms about personal information dissemination for the online context. Section 2 argues that the disclosure, dissemination, and processing of personal information are rife with issues of self control. Section 3 analyzes personal information norms in light of these issues. In particular, Section 3 discusses why socially beneficial personal information norms will probably not develop to deal with widespread computerized data processing and argues that people will likely disclose more personal information online than is consistent with their long-term preferences. Failures of the “market” for personal information, which are mitigated by social norms in the interpersonal context, thus must be addressed by other means. Section 4 discusses whether and how legal regulation should address these norm failures. Care must be taken in devising such regulations in light of the personal autonomy questions that are inevitably raised by regulations that respond to issues of self-control.

## **2. PERSONAL INFORMATION AND SELF CONTROL**

The disclosure and dissemination of personal information about individuals within a community has traditionally been regulated by a nuanced system of social norms. Social norms regulate prying and gossip and also the “inappropriate” disclosure of certain kinds of personal information in certain contexts. By and large the function of these personal information norms has yet to be analyzed in depth from a social norms theory perspective.<sup>2</sup> Yet the question is important for at least two reasons.

<sup>1</sup> Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, RUTGERS L. REV. (forthcoming 2005).

<sup>2</sup> Richard H. McAdams, *The Origin, Development and Regulation of Norms*, 96 MICH. L. REV. 338, 424-33 (1997), has analyzed the effects that restricting the dissemination of personal information through privacy might have on the evolution of social norms. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 838-43 (2000), has discussed how information privacy might mitigate some of the harmful effects of overly zealous enforcement of social norms. Steven A. Hetcher, *NORMS IN A WIRED WORLD* 243-305 (2004), has devoted considerable attention to the emergence and function of social norms that govern the behavior of online website owners, but has not applied the analysis to interpersonal dissemination and disclosure of personal information.

First, since social norms often arise out of underlying conflicts between individual preferences and collective benefits,<sup>3</sup> they provide clues to those underlying conflicts. Studying them may bring to light social issues that need to be addressed in contexts in which norms are ineffective. Second, many have mourned a perceived decline in social norms about personal information disclosure<sup>4</sup> and predicted that modern data processing and other technological means for obtaining personal information will lead to major and undesirable social changes.<sup>5</sup> To understand whether these social forces will result in a breakdown of personal information norms – and to determine whether such a breakdown is a problem that should be addressed by legal regulation – it is important to try to understand these norms and to see what underlying social purposes they have served.

In this chapter, I argue that many personal information norms are best understood as “willpower norms,” which are social norms aimed at compensating for human failures of rationality and self-control. Willpower norms arise in the personal information context because both disclosing information and obtaining information are subject to problems of self control and temptation. Individuals regularly both disclose information they wish they had not disclosed and obtain information they are unable to consider rationally, with resulting social disutility. Personal information norms can curb these tendencies by reinforcing the self-control of both disclosers and recipients of the information.<sup>6</sup>

Though a large fraction of social discourse consists of discussion of the activities – including the follies and foibles – of friends, colleagues, and acquaintances, there are well-recognized boundaries to the types of personal information that can “appropriately” be discussed. The boundaries depend on the identities of the participants in the conversation. Most interesting – and puzzling – are social norms opposing disclosure of one’s own personal information to others. Even in today’s “tell-all” society (or perhaps especially so), there is widespread aversion to and disapproval of the disclosure of personal information at the wrong time and place. It is not

<sup>3</sup> See, e.g., Hetcher, *supra* note 2 at 38-78, for a review of social norm theory.

<sup>4</sup> See, e.g., Rochelle Gurstein, *THE REPEAL OF RETICENCE: A HISTORY OF AMERICA'S CULTURAL AND LEGAL STRUGGLES OVER FREE SPEECH, OBSCENITY, SEXUAL LIBERATION, AND MODERN ART* (1996); Anita L. Allen, *The Wanted Gaze: Accountability for Interpersonal Conduct at Work*, 89 *GEO. L. REV.* 2013 (2001); Anita L. Allen, *Coercing Privacy*, 40 *WM. AND MARY L. REV.* 723 (1999) for arguments that the widespread “waiver” of privacy by individuals is a social problem.

<sup>5</sup> See, e.g., Daniel J. Solove, *THE DIGITAL PERSON* (2004), and references therein.

<sup>6</sup> Unfortunately, personal information norms can also serve as socially pernicious and inefficient “silencing norms,” as exemplified by the “don’t ask, don’t tell” policy against gays in the military. This possibility is analyzed in Strandburg, *supra* note 1.

simply that individuals do not want to share everything with everyone, but also that *individuals do not want to know everything about everyone else*.<sup>7</sup>

These social norms against providing information are puzzling when one stops to think about it, especially in light of the high value usually placed by society on the free flow of information. The availability of information is an assumed prerequisite to a well-functioning and efficient marketplace. In addition, transparency is a widely held democratic value and the ability to obtain and discuss information about others is considered by many to be an important aspect of free speech.<sup>8</sup> If personal information disclosures were always valuable to the recipients of the information, it is difficult to see how social norms against disclosing personal information could arise.

## **2.1 Self-Control Issues in Personal Information Disclosure and Dissemination**

Both disclosing one's own personal information and obtaining personal information about other people can raise self control issues. Moreover, there can be social costs when people yield to the temptation to disclose or to obtain personal information.

### **2.1.1 Temptations to Disclose Personal Information**

People often disclose personal information despite having indicated a preference for keeping such information private. This tendency has been documented particularly well in the context of online disclosures. In the past few years, a large number of surveys and a few experimental studies have probed public attitudes about online disclosure of personal information.<sup>9</sup>

<sup>7</sup> See Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure*, 53 DUKE L. J. 967, 1035-44 (2003), noting that more information can lead to misjudgment because information is taken out of context and because of irrational judgments based on stigmas; and Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 at 1403-04, arguing against the contention that more information always leads to more knowledge.

<sup>8</sup> For example, Eugene Volokh has characterized the right to information privacy as a "right to stop you from speaking about me." Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1117 (2000). Volokh analyzes various rationales for permitting the subject of personal information to control its dissemination and argues all could be expanded easily to justify restricting other types of discourse. See also Diane L. Zimmerman, 68 CORNELL L. REV. 291, 326-36 (1983), discussing tensions between the privacy torts and constitutional values and also arguing that gossip serves a positive function.

<sup>9</sup> For a very useful bibliography of surveys of the American public regarding privacy issues, see Bibliography of Surveys of the U.S. Public, 1970-2003

Respondents generally report a high degree of concern about the privacy of their personal information<sup>10</sup> and strongly believe that they should have control over its use. However, as noted by Stan Karas, “despite warnings against personality-warping self-censorship, there exists little evidence that consumers actually alter their behavior because of ongoing data collection.”<sup>11</sup> And few individuals take affirmative steps to protect their online privacy.<sup>12</sup> In other words, despite having indicated a preference not to disclose personal information online, individuals in fact disclose such information frequently.

One possible conclusion from these studies would be that people are simply not as concerned about revealing their personal information in the course of real transactions as they report themselves to be when considering a disclosure in the abstract. However, a very interesting study by Sarah Spiekermann and collaborators suggests another possibility. The study probed the correspondence between subjects’ reported privacy concerns and their behavior during an online shopping trip involving real purchases.<sup>13</sup> The study involved an online “bot” named Luci which asked the shoppers a variety of personal questions to guide their product selection. The subjects’ behavior during the shopping trip seemed inconsistent with reported privacy preferences. All participants, including those who reported strong privacy preferences, answered a high number of the “Luci’s” personal questions.

A closer inspection of the participants’ behavior brought to light correlations between shopping behavior and reported privacy preferences, however. Those study participants who had expressed greater privacy concerns delayed answering the bot’s questions, checking frequently to see whether an information search would provide a satisfactory recommendation for their purchase, such that answering the question could be avoided. Though many of them eventually revealed nearly as much personal information as those ostensibly less concerned with privacy, they thus appeared to be much more conflicted about providing the personal information that was requested, providing it only after a period of delay.

These experiments suggest that the more privacy-conscious individuals engaged in an internal struggle over whether to reveal the information. If

at <http://www.privacyexchange.org/iss/surveys/surveybibliography603.pdf>.

<sup>10</sup> See, e.g., Susannah Fox, *Trust and Privacy Online: Why Americans Want to Rewrite the Rule* (2000).

<sup>11</sup> Stan Karas, *Privacy, Identity, and Databases*, 52 AM. U. L. REV. 393, 414 (2002).

<sup>12</sup> A. Acquisti and J. Grossklags, *Losses, Gains and Hyperbolic Discounting: An Experimental Approach to Information Security and Behavior*, in *THE ECONOMICS OF INFORMATION SECURITY* (L.J. Camp and S. Lewis, eds., 2004) at 165-178, reviewing and citing surveys.

<sup>13</sup> Sarah Spiekermann, Jens Grossklags, and Bertina Berendt, *E-Privacy in 2<sup>nd</sup> Generation E-Commerce: Privacy Preferences v. Actual Behavior*, in *3RD ACM CONFERENCE ON ELECTRONIC COMMERCE - EC '01* (2002).

this speculation is correct, the study may provide evidence that the inconsistency between individuals' stated attitudes about disclosing personal information and their behavior is a result of struggles pitting long term desires for privacy against short term temptations to disclose information in exchange for relatively minor, but immediately attractive, savings or conveniences. As recognized in a recent economic treatment of information privacy online, "the protection against one's own future lack of willpower could be a crucial aspect [of] providing a link between information security attitudes and actual behavior."<sup>14</sup>

Temptations to disclose personal information may arise not only from the opportunity to trade privacy for immediate gain, as in the usual online context, but from a taste for the disclosure itself. Of course, much of the personal information that provokes concern when it is disclosed in commercial transactions seems unlikely to be the subject of such a taste for disclosure. Likely few people get an inherent kick out of disclosing their credit card numbers or social security numbers. However, the issue of personal information disclosure is significant in many arenas other than commercial transactions. Disclosure of personal information is at issue in social, employment, health care and other contexts in which an inherent appetite for expression is much more likely to come into play.

In summary, individuals demonstrate ambivalent attitudes and behavior with respect to disclosing their own personal information, suggesting that time-inconsistent preferences and self-control may have important ramifications for personal information disclosure.<sup>15</sup>

### **2.1.2 Self-Control Issues with Obtaining and Handling Personal Information about Others**

It is relatively easy to understand why people might wish to obtain personal information about others. Such information may be directly useful in evaluating the advisability of transacting with them, might even provide opportunities to exploit or defraud them, might be indirectly useful as a kind

<sup>14</sup> Acquisti and Grossklags, *supra* note 12.

<sup>15</sup> These issues of temptation and willpower arise in addition to other related concerns. Individuals may not make good decisions about whether to disclose personal information for a variety of reasons beyond lack of self-control. *See, e.g.,* Alessandro Acquisti and Jens Grossklags, *Privacy and Rationality: Preliminary Evidence from Pilot Data*, 3RD ANNUAL WORKSHOP ON ECONOMICS AND INFORMATION SECURITY at 3 (WEIS 2004); Acquisti and Grossklags, *supra* note 12; Schwartz, *supra* note 2. *See generally,* Daniel Kahneman and Amos Tversky, eds., *CHOICES, VALUES, AND FRAMES* (2000) for a review of "bounded rationality."

of “morality tale” about the costs and benefits of particular lifestyle choices, and might satisfy a simple curiosity or taste for information about others.

Despite the obvious potential to benefit from obtaining personal information about others, it is well known that individuals sometimes obtain information against their better judgment. Many have experienced regret at having yielded to the temptation to read a letter carelessly left out on a desk or an unintentionally forwarded email. As noted by Solove, “Similarly, people may recognize the value of being restrained from learning certain details about others, even if they crave gossip and would gain much pleasure from hearing it.”<sup>16</sup> Elsewhere, I analyze in detail why this might be the case.<sup>17</sup> The analysis has three steps: (1) explaining that people might make better decisions if they avoid certain information because the accuracy of decisionmaking does not always increase with increasing information availability and because people exhibit systematic irrationalities in information processing, including a tendency to over-emphasize certain distracting information; (2) arguing that people experience self-control problems about obtaining and considering such information; and (3) arguing that personal information is particularly likely to be the object of such problems because it is often highly contextual and tends to be distracting.

The conclusion from this analysis is that we should not be surprised if people have complex preferences about learning personal information about others. Such information is likely to be useful and interesting in some contexts and distracting and confusing in others. Frequently, personal information about others is interesting in the short term but distracting or confusing in the long run, leading to the time-inconsistent preferences about nosing into other people’s affairs that are familiar from daily life. These complicated time-inconsistent preferences about personal information may underlie the complex social regulation of personal information dissemination by personal information norms.

### **3. PERSONAL INFORMATION NORMS AS WILLPOWER NORMS**

Because the short-term and long-term costs and benefits of disclosing and obtaining personal information are highly dependent on the context of the disclosure, it is not surprising that personal information norms are highly contextual. While a detailed analysis of such norms is beyond the empirical

<sup>16</sup> Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure*, 53 DUKE L. J. 967, 1050 (2003).

<sup>17</sup> Strandburg, *supra* note 1.

foundation of this chapter, it is possible to make some general arguments about these norms based on the concept of “willpower norms.” I also give a more detailed analysis of the online disclosure of personal information, a context in which personal information norms can be ineffective.

### 3.1 Norms against Disclosing Personal Information

Under the traditional view that more information is better, one would expect self-disclosures to be welcomed and reticence to be suspect. As explained by Professor Richard Murphy: “in grossly oversimplified terms, the consensus of the law and economics literature is this: more information is better, and restrictions on the flow of information in the name of privacy are generally not social wealth maximizing, because they inhibit decision-making, increase transaction costs, and encourage fraud.”<sup>18</sup> Those who wish to keep others from obtaining personal information about them are suspected of seeking to exploit third party misapprehensions.<sup>19</sup>

If one accepts that both disclosing and receiving personal information are subject to self control failures, however, it is much easier to understand the phenomenon of norms against disclosing information. Individuals’ long-term incentives both as disclosers and recipients of information could then motivate them to participate in penalizing the disclosure of “inappropriate” personal information. Norms against disclosing certain types of personal information in certain contexts can compensate for common cognitive and self-control problems related to the taste for disclosure and for inquiry, the likely irrelevance of personal information, and the difficulty in properly processing – or ignoring – distracting information. Because the extent to which information is “more prejudicial than probative” will vary according to the context, the norms of disclosure can be expected to vary accordingly. Information that is considered “inappropriate” in one context might be considered a perfectly acceptable subject of disclosure in another. For example, norms cordoning off the disclosure and dissemination of certain types of personal information in environments such as the workplace may be explicable on these grounds. If personal information is “floating around” the office it may be imposed on those who would prefer not to know it.

To summarize, the willpower norms concept is helpful in understanding why personal information norms prohibit both disclosing and prying into personal information in some circumstances. When disclosers and hearers are more or less similarly situated members of a close-knit community, these

<sup>18</sup> Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2382 (1996).

<sup>19</sup> See Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 399-400 (1977-78).

personal information norms will often be socially beneficial and efficient as ways of coping with common human weaknesses.<sup>20</sup> Deviations from these norms will frequently be detectable and can be punished with social disfavor. The next sub-section asks whether and how personal information norms will function in the context of online disclosures.

### **3.2 Personal Information Norms and the Disclosure of Personal Information Online**

Disclosure of personal information online can be analyzed as a willpower issue.<sup>21</sup> Individuals may disclose personal information in transactions with websites – even, for example, when those websites do not have effective privacy controls – because the temptation of immediate gratification overcomes a longer-term preference not to disclose such information. Will social norms arise to compensate for such self-control failures? The development of social norms generally requires a repeatedly-interacting group, which is able to detect and penalize deviations from the norm. These conditions may not be satisfied in the online context. To explore this question, it is helpful to distinguish two contexts for personal information disclosure: the online community and the online commercial transaction.

#### **3.2.1 Personal Information Norms and Online Communities**

Online communities are groups of individuals who interact on an interpersonal level over the internet. These interactions take place in various venues, including chat rooms, listserves, bulletin boards, and so forth. There may be some question about whether online communities can develop personal information norms, since participants are often identified only by screen names and the social displeasure of the online group cannot easily penetrate into the “real world” context. However, online communities often do develop informal norms about disclosure of personal information.<sup>22</sup> Moreover, if norms fail to develop, such communities often promulgate rules of behavior, enforced by a central authority, to regulate personal information

<sup>20</sup> In Strandburg, *supra* note 1, I discuss how personal information norms may go awry, leading to pernicious effects on minority groups and impeding the evolution of norms about other types of behavior.

<sup>21</sup> See Alessandro Acquisti, [Privacy in Electronic Commerce and the Economics of Immediate Gratification](#), in PROCEEDINGS OF ACM ELECTRONIC COMMERCE CONFERENCE (EC 04) (2004), and Acquisti and Grossklags, *supra* note 12, for explorations of this possibility from a behavioral economics perspective.

<sup>22</sup> See, e.g., Uta Pankoke-Babatz and Phillip Jeffrey, *Documented Norms and Conventions on the Internet*, 14 INT’L J. HUMAN-COMPUTER INTERACTION 219 (2002).

disclosure, among other things. Such codes of “netiquette” are increasingly common. To the extent that group members value their online interactions, they are susceptible to reputational and shunning penalties for “inappropriate” behavior just as people are in the offline world.

Even if netiquettes develop, however, two factors make personal information norms less effective in such online communities than in real world communities. First, if online conversations are maintained in a searchable archive (as they may be either intentionally or unintentionally by the website owner), personal information may “escape” from the community in which it was disclosed to contexts in which it will not be correctly understood. The community’s norms may not account for this possibility, especially if the archiving is invisible to participants. Second, such online communities may have corporate sponsors, who are silent observers of the interpersonal exchange and may also communicate the information beyond the community. These corporate sponsors may not be constrained by community norms about disclosure if their norm violations are not visible to the group. Moreover, they may in some instances have access to information that maps an online identity to a real world identity. For these reasons, personal information norms may fail to deter some undesirable secondary disclosures of personal information.

### **3.2.2 Personal Information Norms and Commercial Transactions**

In the commercial online context, norms governing personal information disclosures are difficult to establish. One consumer’s disclosure of or failure to disclose personal information in an online transaction is of no direct interest to other consumers since they are not the recipients of the information.<sup>23</sup> I argue elsewhere that a willpower norm might develop even around behavior that does not affect other people because a repeatedly interacting group can assume reciprocal obligations to punish common lapses of self-control.<sup>24</sup> Online commercial disclosures cannot easily support such a norm, however, both because failures of will are not observed by other online consumers and because online consumers do not form a repeatedly interacting group.

While consumers are unable to develop a norm of penalizing one another for excessive online disclosures of personal information, they do have ways to penalize “tempters” – in this case websites without protective privacy

<sup>23</sup> This is not strictly true, since consumers share a common interest, as explored by Hetcher, *supra* note 2, at 258-59, and discussed below, in pressuring websites to change their data collection policies.

<sup>24</sup> Strandburg, *supra* note 1.

policies which offer immediate commercial gratification in exchange for personal information disclosures which may be regretted later. For example, online consumers could punish such websites for failing to protect privacy by boycotting them. Is a norm against dealing with such websites likely to arise? Professor Steven Hetcher argues that consumers face a collective action problem in attempting to influence website companies to adopt more privacy-protective policies.<sup>25</sup> Consumers as a whole might be better off refusing to deal with sites that do not offer a high level of privacy protection, but for each individual consumer it is rational to attempt to free ride on the boycott efforts of others. Unlike consumers in the offline world, who can enforce boycotts by observing when people deal with “forbidden” retailers, online consumers are unable to enforce a boycott based on a website’s privacy policies because they cannot detect and penalize defectors. This analysis suggests that consumers will not be able to sustain a “norm against tempters” that penalizes such websites.

However, as discussed in detail elsewhere,<sup>26</sup> the self control context provides a mechanism that may permit social norms to influence unobservable behavior. One personal mechanism for enhancing self control is to categorize or “bundle” behaviors using personal rules.<sup>27</sup> Willpower norms can reinforce such individual self control measures by operating to “bundle” undetectable behaviors with socially disfavored detectable behaviors. Because an individual may perceive that her *undetectable* violation of a rule signals that she is also likely to violate the rule *in public*, “bundling” provides a mechanism by which social norms can influence undetectable behavior. In the online context, for example, if a consumer were to categorize online personal information disclosures with inappropriate *public* disclosures of personal information as part of a personal rule, her ability to resist the temptation to disclose online could increase.

In fact, Hetcher’s description of the activities of “norm entrepreneurs” in the context of website privacy policies may be evidence of just such a bundling willpower norm. Hetcher details how norm entrepreneurs created a consumer demand for online information privacy in part by moralizing the meaning of online data collection by re-categorizing data collection as a

<sup>25</sup> Hetcher also discusses in detail why a functioning market for privacy-protective policies may fail to develop. *Supra* note 2 at 243-60.

<sup>26</sup> Strandburg, *supra* note 1.

<sup>27</sup> See, e.g., Drazen Prelec and Ronit Bodner, *Self-Signaling and Self-Control* in TIME AND DECISION (George Loewenstein *et al.*, eds., 2003), arguing that activities with low marginal efficacy, such as voting, may be explained as signals to the self of future propensity to resist temptation. Such a propensity increases the attractiveness of resisting temptation now. See also George Ainslie, BREAKDOWN OF WILL 90-104 (2001), at 90-104.

privacy invasion.<sup>28</sup> Norm entrepreneurs framed the behavior of websites that do not protect privacy as “disrespectful.” It is not immediately clear from Hetcher’s description, however, why framing behavior as “disrespectful” will help to solve the consumer collective action problem. Consumers can free ride on the efforts of others to boycott “disrespectful” websites just as easily as on efforts to boycott privacy-invasive websites. The answer may lie in the “bundling” self-control strategy just discussed. The moralizing of privacy policies has the effect of re-framing “dealing with a website that does not provide privacy protection” as “allowing oneself to be treated with disrespect.” Dealing with such a website then becomes just one of many ways in which an individual might violate a personal rule that says “I do not allow myself to be treated with disrespect.” Bundling the undetectable online behavior of “dealing with websites that do not protect privacy” with more detectable instances of being treated with disrespect has the potential to aid the individual in resisting the temptation to deal with those websites.<sup>29</sup>

### **3.3 Implications of Personal Information Norms for Computerized Data Processing**

#### **3.3.1 Computerized Data Processing and the Relevance of Personal Information Norms**

Jange and Schwartz define “information privacy” as “the creation and maintenance of rules that structure and limit access to and use of personal data.” They note that the rules are sometimes found in norms, such as those involving gossip, and sometimes in law.<sup>30</sup> Under this definition, an understanding of personal information norms would seem central to an understanding of information privacy. It may thus be a bit surprising that rather minimal attention has been paid to the theory of personal information norms in the information privacy debate. This relative inattention to the norms that govern the interpersonal flow of personal data is not as surprising, however, when one considers that much of the focus of recent discussions of information privacy rightly has been on analyzing the impact of computerized data processing and collection by corporate entities.

Social norms of the sort analyzed here do not govern the behavior of these commercial entities directly. One may thus ask whether social norm

<sup>28</sup> Hetcher, *supra* note 2, at 268-72.

<sup>29</sup> Whether such a norm can be effective when websites have deceptive privacy policies is another question, of course.

<sup>30</sup> Edward J. Jange and Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1223 (2002).

analysis has anything to add to the debate about the regulation of commercial applications of computerized data processing. However, the relevance of personal information norms to this debate stems in part from the very fact that these entities are not subject to social norms. In today's society, the flow of personal information is less and less subject to social norm mechanisms of enforcement: disclosures are often made in unobservable online contexts; information is disseminated to and by corporate entities; and information flow is no longer confined to a community of individuals who interact repeatedly. This social norm failure can be beneficial in some instances, by undermining silencing norms and permitting minority group discourse. However, it also seems likely that social norms will no longer be able to mitigate the effects of bounded rationality and willpower in cases where long-term preferences would counsel against disclosure. Moreover, where, as is usual in the online context, disclosures are made to corporate entities, there is the danger that those entities will develop their own norms that promote their private interests but are socially detrimental. For example, Hetcher has argued that websites are likely to develop a coordination norm of deceptive privacy practices, while individuals will have difficulty developing and enforcing norms of privacy-protective behavior.<sup>31</sup>

Unless other self-control mechanisms are available, one may thus expect individuals to disclose significantly more information in the online context than they would prefer to disclose in the long term. At the same time, computerized data processing permits far more extensive aggregation and dissemination of personal information than is possible in the interpersonal context. Roger Clarke coined the term "dataveillance" to describe the monitoring of individual behavior that is made possible by computerized data collection.<sup>32</sup> Professor Julie Cohen argues that data collection reduces autonomy because it provides a means of informational surveillance which generates "a 'picture' that, in some respects, is more detailed and intimate than that produced by visual observation."<sup>33</sup> Data may be aggregated over space and time and may be searched to discern patterns.

Data aggregation exacerbates the self-control issues that affect decisions to disclose personal information. Disclosure of each piece of information is particularly tempting because each disclosure forms an insignificant part of the picture. Personal information may also be disseminated far more rapidly

<sup>31</sup> Hetcher, *supra* note 2 at 255-58.

<sup>32</sup> See Roger Clarke, *Information Technology and Dataveillance*, 315 COMMUN. ACM 498 (1988).

<sup>33</sup> See Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425 (2000).

and widely by computer than is likely in the interpersonal context, to parties that have no contextual knowledge of the individual involved. This widespread and rapid dissemination makes it difficult, if not impossible, for individuals to make rational predictions of the costs and benefits of each disclosure. As explained in a recent economic treatment, “[T]he negative utility coming from future potential misuses of somebody’s personal information is a random shock whose probability and scope are extremely variable . . . [the] individual [] is facing risks whose amounts are distributed between zero and possibly large (but mostly uncertain) amounts according to mostly unknown functions.”<sup>34</sup>

One might argue that concern about this increased circulation of personal information should be mitigated by the fact that the human failings of rationality and will that were central to our explanation of personal information norms are not at issue in computerized data processing. Thus, the argument would go, commercial entities will process information rationally and, though individuals may not like the outcome of that rational decision-making, society will not suffer when individuals disclose more personal information than they might in the long run prefer.

There are many reasons to criticize this hypothesis. I discuss two reasons here. First, it may be privately advantageous for online data collectors to use personal information in socially suboptimal ways and the market will fail to correct this tendency. Second, it is a mistake to assume that computerized data processing entities are immune from human failings in interpreting personal information. Inescapably, decisions about what data to collect and how to analyze it are made by human beings.

### **3.3.2 Information Externalities and Computerized Information Processing**

As has become increasingly evident, commercial entities may prefer to collect more information and to be less careful about its security than is socially optimal for a variety of reasons.<sup>35</sup> Most importantly, the collecting entity does not bear the full cost of privacy losses to the subjects of the information, including any costs that arise from criminal misuse of the information by rogue employees or hackers or from errors in the data. Because of their own self-control failures and inability to take into account

<sup>34</sup> Acquisti and Grossklags, *supra* note 12.

<sup>35</sup> For a more formal economic treatment of the incentives of private firms to obtain inefficient amounts of information, see Curtis R. Taylor, *Privacy in competitive markets* (Technical report, Department of Economics, Duke University, 2004), available at <http://www.econ.duke.edu/Papers/Other/Taylor/privacy.pdf>.

accurately the expected costs of disclosing personal information online, individuals will not force these entities to pay a high enough “price” for personal information. Thus, the personal information “market” will not solve this problem.<sup>36</sup> Recent high-profile demonstrations of insufficient information security may well lead to improved legal regulation aimed at curbing the possibility of malicious uses of personal information.<sup>37</sup> Such regulation raises few concerns about paternalism – not many individuals have long-term preferences for insecure or inaccurate data collection!

The self-control analysis highlights a further way in which rational uses of data processing may lead to socially harmful results, however. Targeted marketing, based on the analysis of consumer buying patterns, has the apparent potential for great social benefit. It promises to eliminate social and consumer waste associated with marketing that is aimed at those who have no interest in the services or products being offered. Despite these reasonable-sounding justifications, there is widespread uneasiness with the idea that commercial entities might base their marketing on personal profiles that are too detailed or complete. This uneasiness is somewhat mysterious if consumers are rational processors of marketing information. Presumably, everyone could be subjected to less advertising if the advertising could be targeted accurately. If, however, one accounts for the influence of temptation and willpower on consumption decisions, the aversion to overly personalized marketing makes more sense. A more detailed personal profile permits a more targeted satisfaction of consumer preferences, but also a more targeted attack on consumer will. The possibility that targeted advertising can undermine long-term preferences may explain an intuition that such detailed profiling is a threat to personal autonomy. This analysis suggests that consumer antipathy to spam and pop-up ads, for example, may be premised on more than concerns about attention consumption.<sup>38</sup>

<sup>36</sup> See Jange and Schwartz, *supra* note 30, at 1241-46, making the point that because of bounded rationality the privacy market between financial institutions and consumers does not function well.

<sup>37</sup> See, e.g., *Some Sympathy for Paris Hilton*, New York Times Week in Review, February 27, 2005, discussing various personal information leaks, including the recent leak of personal information about 145,000 individuals by Choicepoint; *FTC Drops Probe into DoubleClick Privacy Practices*, CNET News.com, January 22, 2001 at <http://news.com.com/2100-1023-251325.html?legacy=cnet>, describing the “maelstrom of scrutiny from consumer advocates, media and legislators about data-collection practices on the Web” set off by an announcement of plans to combine online “clickstream” data with personally identifiable information for advertising purposes.

<sup>38</sup> See Eric Goldman, *Data Mining and Attention Consumption*, in this volume, for an analysis of targeted marketing based on its costs in attention consumption.

### 3.3.3 Rationality, Willpower, and Computerized Data Processing

Computerized data processing may also not be immune from the irrationalities that affect human processing and interpretation of personal information. Are individuals correct to fear that computerized processing of personal information will be used to make bad decisions about them? Or are they simply seeking to benefit from hiding negative information about themselves from their employers, insurance companies, and potential dates?

Computers, one may safely say, are not plagued by issues of temptation and self-control. They are neither curious nor confessional. They simply do what they are told. Thus, the relevance of bounded rationality and willpower to computerized data processing stems from three things: human choices affecting the input data; human choices about how to process the data; and human interpretation of the computerized analysis. Computerized uses of personal information can range from the simple collection of a mailing list to sophisticated and innovative techniques for “mining” patterns from large quantities of data. It is beyond the scope of this chapter to provide an extensive analysis of the ways in which these various uses of computer analysis might fall prey to bounded rationality and limited self-control. However, the potential pitfalls may be illustrated by a few specific points.

First, corporate entities may tend to over-collect information if the costs associated with processing excessive information are not imposed on the group within the entity that makes decisions about collection. Collecting more data may impose very minor immediate costs. Failing to collect and store the data may implicate loss aversion, resulting in a tendency to avoid the greater regret that might accompany an irretrievably lost opportunity to acquire information (particularly because information – especially in digital form – seems very easy to “throw away later.”)<sup>39</sup> Moreover, the individuals in charge of data collection may perceive (probably correctly) that they will suffer more dire personal consequences if they fail to collect data than if they collect an excess of data.

Second, where statistically based techniques are used to categorize individuals based on computerized data, the categorizations may be highly dependent upon the choice of input data and on judgment calls as to when a categorization is “sensible” and when the application of a particular technique (of which there are many) is “successful.” Texts on data mining stress the importance of user input at many stages of the process, including

<sup>39</sup> See, e.g., Russell Korobkin, *The Endowment Effect and Legal Analysis*, *Symposium on Empirical Legal Realism: A New Social Scientific Assessment of Law and Human Behavior*, 97 NW. U.L. REV. 1227 (2003). Of course, the low cost of data collection and disposal also figures into the rational calculus of how much information to collect and raises the rational limit.

selecting data to be used in the data mining computation and assessing the meaning and “interestingness” of patterns that are discovered by the data mining process.<sup>40</sup> Human cognitive limitations can enter at any of these points. Moreover, as a technical matter, computerized data analysis often depends on numerical optimization techniques that are not guaranteed to reach a global optimum. For such techniques, the inclusion of irrelevant information can lead the computation to become “stuck” in a local optimum. Often there are no objective methods for assessing whether a particular data mining result is even close to a global optimum.

Finally, when human decision-makers assess the output of any computerized data analysis, there are several cognitive biases that may come into play. There is a tendency to treat quantitative output as more certain and more objective than may be justified by its accuracy and the amount of subjective input on which it depends. The specificity of numerical output may also give it a salience that could lead to over-reliance on this information. Moreover, the results of computerized data analysis techniques are frequently statistical, giving probabilities that certain correlations or patterns of behavior apply to certain individuals. Even setting aside the normative issue of whether it is fair to make decisions about individuals based on statistical assessments, the well-established difficulties that people have in accurately reasoning based on uncertain, probabilistic information are likely to degrade the assessment of the output of computerized data analysis of personal information.

This subject clearly warrants more extensive treatment. However, the brief discussion here should serve as a warning against any facile assumption that computerized analysis is immune to the limitations of human information processing.

#### **4. PERSONAL INFORMATION NORMS AND INFORMATION PRIVACY REGULATION**

Underlying the debate about the social benefits of information privacy and information flow is the question of the extent to which information privacy is a matter for government regulation rather than individual action, social norms, and market forces. The fact that privacy has benefits and disclosure has costs is not, in and of itself, a justification for government action. Generally, individuals in American society are left to judge for

<sup>40</sup> See, e.g., Jiawei Han and Micheline Kamber, *DATA MINING: CONCEPTS AND TECHNIQUES* 1-34 (2001).

themselves the desirability of engaging in activities that involve tradeoffs of costs and benefits. Government action may be justified, though, when pursuit of individual objectives leads to societal difficulties, including market failures of various sorts.

Here, the personal information norm analysis is instructive. The very existence of social norms governing personal information disclosure and dissemination is a red flag that indicates some underlying difficulty with purely individual decisions about when to disclose and disseminate personal information. Understanding the provenance of personal information norms thus provides clues as to whether legal regulation or other government intervention is likely to be appropriate. The analysis of personal information norms in this chapter thus has implications for the debate about information privacy regulation. In this section I provide a preliminary discussion of some implications for the debate about information privacy regulation in the context of computerized data processing.

First, the recognition that disclosing and obtaining personal information are subject to self control problems undermines the facile assumption that individual decisions to disclose or obtain such information reveal long-term preferences about information privacy. It also supports arguments that information privacy is not a simple tradeoff between privacy's benefits to subjects of the information and costs to others of being deprived of the information. Information privacy regulation has the potential for direct benefit both to subjects and to recipients of information. On the other hand, while providing additional justification for privacy regulation, the personal information norms analysis also highlights potential dangers of such regulation. As with other attempts to regulate behavior that is subject to temptation, the prospect of interfering with individual liberty must be taken seriously, since it is difficult to distinguish time-inconsistent preferences from either true minority preferences or long-term preference changes.

Second, where individual self-control measures fail and social norms are ineffective for some reason (such as where there is no close-knit community to enforce them or where violations are undetectable), legal regulation may promote the long-term social good. For example, as already discussed, modern technology may undermine the effectiveness of personal information norms in many instances. Yet the temptations associated with disclosing and disseminating personal information persist. A market approach to information privacy will not work in such circumstances. Regulation may be desirable to replace the social norms that have historically mitigated market failure in the interpersonal context.

There are serious hazards, however, to employing legal regulation to bolster self-control. As I argue in detail elsewhere,<sup>41</sup> the willpower norms analysis suggests that the use of the law in a paternalistic way to enforce self-control should be approached with care because of the possibility of imposing “silencing norms” on minority groups, of masking norm changes, and of other impositions on the liberty of those whose long-term preferences differ from those of the majority. The best approach thus may be to structure the law to support voluntary self-control measures whenever possible. Mechanisms for promoting information privacy should be designed as much as possible to permit individuals to distinguish for themselves between long term preferences and short term temptations. Usually this will mean enhancing – and perhaps mandating – the availability of self-control measures, while permitting individuals to “opt out” of those measures.

#### **4.1 Personal Information Norms and the Legal Regulation of Online Communities**

In the interpersonal context, legal strictures against disclosing one’s own personal information to other individuals are likely to be unnecessary, intrusive, and insufficiently in tune with particular webs of interpersonal relationships. Section 3.2.1 identified two situations in which personal information norms may fail to function in online communities. Both concerned the behavior of those who obtain personal information “incidentally” rather than as participants in the online discussion.

One approach to these potential norm failures in online communities might be to require that websites providing interpersonal discussion for a give clear notice of their policies about archiving the online discussion and about corporate use of information disclosed in the discussions. Because community members have repeated interactions with each other and with the website owners, notice may be enough to permit online communities to subject these owners to community norms about the treatment of personal information.

Another approach would be to subject website owners to tort liability to the extent that their behavior violates the social norms that pertain to other members of the online community. I argue elsewhere<sup>42</sup> that the interpretation of reasonable expectations of limited privacy in the tort law context should take into account the social norms of the group in which the

<sup>41</sup> Strandburg, *supra* note 1.

<sup>42</sup> Strandburg, *supra* note 1.

disclosure occurred. This approach may be usefully applied in the context of online social groups. As already discussed, online interpersonal interactions often occur in the context of communities with well-defined social norms or rules about the treatment of personal information. The reasonableness of the behavior of individuals or corporate entities that “lurk” in the background of these discussions and then disseminate or record information disclosed by community members could be evaluated in light of the norms of those communities. Such an application of the privacy torts might also help control the uses of virtual “individuals” (what have been called “buddy-bots”) which are increasingly capable of engaging in conversations that have the “look and feel” of friendly discourse.<sup>43</sup> Such recent advances in computer marketing technology seem likely to tap more and more into the kind of self-disclosure which seems to be inherently pleasurable, and thus potentially tempting. As online experiences begin more and more to resemble conversations with amiable acquaintances (wearing hidden microphones that feed into computer databases), it may be more and more reasonable to hold these virtual individuals to the standards set by appropriate social norms.

## **4.2 Legal Approaches in the Context of Computerized Data Processing**

Some of the social problems resulting from computerized data processing, such as inadequate accuracy and security, may be best attacked by regulating data handlers directly. Other issues, such as targeted marketing, raise more delicate questions of preserving autonomy while avoiding temptation. To avoid the hazards of imposing majority self-control solutions on individuals who may have a long term preference to disclose personal information, legal solutions to these kinds of problems might focus on providing self-control options for consumers. The law can also seek to regulate “the tempters” – for example by requiring data collectors to provide better notice about what will happen to the personal information that individuals disclose – to increase the likelihood that disclosures of personal information reflect long term preferences.

An example of a possible regulation of this sort in the context of disclosure of personal information might be a statute requiring opt-in

<sup>43</sup> See Ian R. Kerr and Marcus Bornfreund, *Buddy Bots: How Turing's Fast Friends Are Under-Mining Consumer Privacy*, in PRESENCE: TELEOPERATORS AND VIRTUAL ENVIRONMENTS (2005), arguing that virtual reality can now be used “to facilitate extensive, clandestine consumer profiling under the guise of harmless, friendly conversation between avatars and humans.”

policies for websites that collect and disseminate personal information. Such a rule would not prevent anyone from disclosing any personal information, but would assist individuals in resisting the temptation to disclose by aggregating most disclosure decisions under a non-disclosure category and setting that category as the default.<sup>44</sup> Individuals would no doubt still disclose information in many circumstances, but would be required to “justify” each disclosure to themselves as a reasonable “exception” to the default rule of non-disclosure. Perhaps even better would be to mandate that internet service providers provide a choice of “privacy plans” requiring each user to select a customized personal information disclosure “rule” that would apply to online transactions as a default, but could be over-ridden on a case by case basis. Thus, consumers with a long-term preference for disclosure could choose an “opt-in” rule and avoid the transaction costs of opting in in piecemeal fashion.<sup>45</sup> Just as a spam filter takes away the need to consider (and perhaps even be tempted by) unsolicited email advertising, a privacy rule could permit individuals to choose not to be confronted with the possibility of transacting with websites with privacy policies that do not meet pre-selected standards or to choose to have website options for a particular transaction divided into compliant and

<sup>44</sup> See, however, Jange and Schwartz, *supra* note 30 at 1245-59, questioning whether opt-in defaults are sufficient in light of consumer bounded rationality and asymmetrical information. Jange and Schwartz do not consider the role that opt-in defaults might play as self-commitment mechanisms, but their concerns are well-taken. The possibility of a voluntary technologically-implemented privacy rule that removes commercial entities from consideration if they do not comply with pre-set privacy choices may mitigate these concerns to some extent.

<sup>45</sup> The Platform for Privacy Preferences (P3P) provides a standard for machine-readable privacy policies that has been implemented on many websites. Lorrie Cranor et al., [An Analysis of P3P Deployment on Commercial, Government, and Children's Web Sites as of May 2003](#), TECH. REP., FEDERAL TRADE COMMISSION WORKSHOP ON TECHNOLOGIES FOR PROTECTING PERSONAL INFORMATION (May 2003). Unfortunately, “P3P user agents available to date have focused on blocking cookies and on providing information about the privacy policy associated with a web page that a user is requesting. Even with these tools, it remains difficult for users to ferret out the web sites that have the best policies.” Simon Byers, [Lorrie Cranor](#), Dave Kormann, and [Patrick McDaniel](#), *Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine*, in PROCEEDINGS OF THE [2004 WORKSHOP ON PRIVACY ENHANCING TECHNOLOGIES \(PET2004\)](#). Given the procrastinations and temptation issues discussed here, automated privacy rules are unlikely to provide significant social value unless they are easy to use. Most recently, a search engine has been developed that displays information about a website’s privacy policy next to its entry in the search results. *Id.* If this feature is widely adopted by well-known search engines, it may dramatically improve the practical effectiveness of the technology. However, making choosing a privacy rule a standard aspect of obtaining internet service should drastically increase the effectiveness of such technologies.

non-compliant categories. While it is possible that a market for such privacy plans will develop – especially as privacy-protective technologies become more user-friendly – the possibility for a socially sub-optimal website coordination norm may counsel in favor of legal intervention.

The law might also increase the salience of the potential costs of disclosing personal information by requiring notice of these potential costs precisely at the point of disclosure (somewhat in the spirit of attaching warning labels to cigarettes). Issues of bounded rationality and self-control highlight the importance of the timing, framing, and placement of information about the potential uses of personal information, suggesting that legal regulation of notice should take these issues into account.

## **5. CONCLUSION**

Self-control and temptation have played a significant role in human society throughout history. Personal information norms, which frown upon disclosing certain kinds of personal information and prying into personal information in certain contexts, are possibly explained as willpower norms that have arisen to deal with bounded rationality and self control problems related to disclosing, disseminating, and processing personal information. Because personal information norms frequently arise to compensate for collective action problems in the dissemination of personal information, they highlight the potential for information market failures that can lead to socially sub-optimal decision-making. Therefore, when situations arise in which personal information norms are expected to be ineffective, such as in the context of computerized data processing, alternative mechanisms, including legal regulation, for addressing these problems must be considered. Potentially useful areas of legal regulation include the adaptation of the reasonable expectation of privacy analysis in the privacy torts to account for the personal information norms of a social group; and measures that increase consumer self-control in the context of online information processing – such as opt-in defaults, the ability to set across-the-board personal information rules, and increasing the salience of information about the hazards of personal information online. Norm entrepreneurship that categorizes online personal information disclosures with “real-space” behavior that is governed by social norms – such as the “moralization” of inadequate website privacy policies as “disrespectful” described by Hetcher – may also promote willpower through the bundling mechanism.

Further analysis, and especially further empirical work aimed at elucidating the role that temptation plays in information disclosure and dissemination, will be necessary to understand the interplay between

personal information norms and information privacy law more completely. The concept of willpower norms should also find useful application outside of the information privacy context.

#### **ACKNOWLEDGEMENTS**

I am grateful to Alessandro Acquisti, Julie Cohen, Eric Goldman, Jay Kesan, Roberta Kwall, Richard McAdams, Joshua Sarnoff, Paul Schwartz, Daniel Solove, Lior Strahilevitz, Diane Zimmerman, the participants in the Works in Progress in Intellectual Property Conference at Boston University on September 10-11, 2004, the participants in the Intellectual Property Scholars Conference on August 3-4, 2004 at DePaul, the attendees at the panel on Privacy, Information, and Speech at the Law and Society Association 2004 Annual Meeting, and the attendees at faculty workshops at DePaul College of Law and Loyola Law School, Los Angeles for helpful comments on earlier versions of this work.