Running head: Privacy and the control paradox

Misplaced Confidences: Privacy and the Control Paradox

Laura Brandimarte[1], Alessandro Acquisti[1], George Loewenstein[1]

Correspondence concerning this article should be addressed to Laura Brandimarte, Heinz College, Hamburg Hall, 4800 Forbes Avenue, Room 3005, Pittsburgh PA 15213. E-mail: lbrandim@andrew.cmu.edu

[1] Carnegie Mellon University

Abstract

We introduce and test the hypothesis that increasing perceived control over the release of private information will decrease individuals' concern about privacy and increase their propensity to disclose sensitive information, even when the objective risks associated with such disclosures do not change or worsen. Three online experiments manipulated participants' control over information release, but not over access and usage by others. The experiments show paradoxical effects whereby increased (decreased) control over the *release* of private information increases (decreases) willingness to publish sensitive information, even when the probability that strangers will access that information stays the same or increases (decreases). Our findings highlight how technologies that make individuals feel more in control over the release of personal information may have the unintended consequence of eliciting greater disclosure of sensitive information.

Keywords: privacy, control, paradox, Web 2.0 applications, online social networks, experimental design, behavioral economics of privacy

People often display a notable inconsistency in concern for privacy. They eagerly disclose intimate facts to others, but are bothered when the same information is circulated without their consent. Many online social networks users willfully reveal even self-incriminating information to others – yet, non-substantive changes in privacy policies can generate widespread protests. What can account for these seemingly contradictory behaviors?

We provide evidence for a paradoxical role of perceived control in individuals' willingness to disclose sensitive information, and argue that this has important consequences for debates about the hazards of privacy violations and the adequacy of existing policies intended to protect privacy. In the privacy literature, control over personal information flows is often constructed as instrumental to privacy protection – so much so that both data holding companies and regulators point to control as key to the solution of contemporary privacy challenges. Yet, we show that "more" control can lead to "less" privacy, in the sense of higher objective risks associated with personal information disclosure.

Prior research has identified control as a determinant of risk perception and risk taking (e.g., Slovic, 1987): people are more willing to take risks, and judge those risks as less severe, when they feel in control. However, perceptions of control are often illusory (Langer, 1975). For example, people feel safer driving than flying, and as a result substitute road for air travel, in part based on the feeling that they have more control when driving. We argue that a similar misleading feeling of control underlies many instances of problematic divulgence of information. Specifically, we argue that people fail to distinguish between two importantly different forms of control that are discussed in the literature on privacy (e.g., Petronio, 2002; Phelps, Nowak & Ferrel, 2000): control over *release* of personal information (the action of willingly sharing some private information with a set of recipients) and control over *access* and *usage* of the

information by others (because the final audience who has access to released information may include third parties who gained indirect access to it, and even the intended recipients may use the information in unpredictable ways). People experience a greater feeling of control when they are able to determine the release of information. However, much as other drivers create uncontrollable risks for vehicle occupants, the recipients of information create uncontrollable risks.

Other empirical studies of the relationships between privacy and control can be found in Xu's (2007), Hoadley, Xu, Lee and Rosson (2010), who show that lower perceived control on personal information is associated with higher privacy concerns, and Acquisti and Gross (2006), who found that Facebook users who were the least concerned about the privacy of the information they posted online explained their lack of concern by noting that they felt in control of the information provided.

Our hypotheses are that (1) perceived control influences people's willingness to reveal personal information, and (2) in judging the extent of control, people tend to focus on issues of release at the expense of issues of access and usage – even though objective risks from disclosure arise from whether and how information is accessed and used, not merely how it is released.

Hypothesis (1) is motivated by several factors. First, higher perceived control reduces perceived risks (Slovic, 1987) – in this case, risks associated with information disclosure – which, in turn, positively affects willingness to disclose. Moreover, similarly to the illusion of control (Langer, 1975) – which makes gamblers feel overconfident and, thus, bet more (Goodie, 2005) – control over information release may render people overconfident about the effects of information revelation, inducing them to reveal more and accept higher risks. Conversely, lack of control over information release triggers privacy concerns, almost as if it was not the public

release of private information *per se* that bothered people, but the fact that they did not have complete control over it. Finally, in the Internet domain, perceived control increases users' trust towards the visited website (Hoffman, Novak & Peralta, 1998), which in turn raises perceived security – and hence, propensity to disclose.

Hypothesis (2) arises from a range of cognitive and motivational factors. On the cognitive side, release of information is what people have control over, so it is natural that individuals focus on it, whereas access and usage involve behaviors by other people. In the same way that people are more likely to bet on answers to easy rather than difficult questions, neglecting the fact that questions that are easy for them will likely be easy also for those they are betting against (Camerer & Lovallo, 1999; Kruger, 1999; Moore & Healy, 2008), people focus on their own actions rather than those of potential information-recipients when judging the risk of divulging information. On the motivational side, access and usage of information by others are uncertain events, distant in time, whereas any benefits from release of information are often immediate and more certain (e.g., immediate feedback from Facebook friends). This reduces the saliency of concerns over information usage by others and, therefore, their influence on the individual's decision (Klein, 1998; Slovic, 1975). Hence, control over release can trump the relative lack of control over access, even though the latter may be a more critical determinant of objective risk.

In combination, hypotheses (1) and (2) lead us to predict the potential for a kind of *control paradox*: Individuals who perceive more control over the release of private information are likely to pay less attention to the accessibility, and consequent usage of the information by others – leading in some cases to increased dissemination of potentially harmful information. Paradoxically, therefore, through a mechanism that runs from perceived control to individual

behavior to consequences, technologies that make individuals feel more in control over the release of personal information can increase their likelihood of suffering harms as a result of disclosures.

To test these hypotheses, we conducted three survey-based experiments with students at a North-American University who were asked questions that varied in sensitivity. Across all experiments, we manipulated participants' feeling of control over the *release* of personal information (decreasing it relative to baseline in Study 1 and 2, and increasing it in Study 3) without the *accessibility* by others of the information they revealed. We focused on a dependent variable common in the experimental literature on privacy and information disclosure (e.g., see Joinson, Woodley, & Reips, 2007; Phelps et al. 2000, and most of the 39 studies reviewed in a meta-analysis by Weisband & Kiesler, 1996): individuals' propensities to respond (or not) to personal questions in a survey. Individuals' willingness to answer personal questions, in turn, has been used as a proxy for their privacy concerns (see, e.g., Frey, 1986; Singer, Hippler, & Schwarz, 1992).

STUDY 1

In Study 1, students were approached by the experimenters, and recruited to participate in a survey, with the promise of snacks when they completed it. In the study, participants were invited to become members of a new campus-wide networking website, to be launched at the end of the semester. The survey contained forty questions about the respondent's life in the city and on campus that varied in intrusiveness. Intrusiveness was measured in an initial survey of a separate sample of students from the same population. Instructions explained that none of the

questions required an answer, but that all answers provided would be part of a profile that would appear on the website, visible to the university community only.

Design

The study was a between-subjects design with two conditions. Subjects in Condition 1 read that a profile would be automatically created for them containing the information they provided, and that this profile would be published online once the website was completed. Subjects in Condition 2 read that half of the profiles created would be randomly selected to be published online. By inserting a random element in the publication process, Condition 2 was intended to decrease subjects' feeling of control over the release of their information.

Note that in Condition 2 the probability of private information being released – and therefore available to strangers – was halved as compared to Condition 1. If the decision to answer was more affected by the level of control over information release than by the actual risks associated with its access and usage, then we would expect participants in Condition 1 to be willing to answer more questions. However, a lower response rate in Condition 2 could also be attributable to diminished motivation to reveal information when it is less likely that the information will be publically viewed. In this case, any benefit from revelation (e.g., desire for fame or attention of others) would be reduced. If this were the case, however, we should observe lower response rates by subjects in Condition 2 to questions that would take more effort to answer (open-ended questions regarding courses attended and enrollment programs). A regression of aggregate word counts for the open-ended questions we included for this purpose in the survey failed to reveal any statistically significant difference across the two conditions, which strongly weighs against this alternative explanation.

Results

Sixty-seven participants were assigned to Condition 1, and 65 to Condition 2. In this and following studies the distribution of age and gender did not differ significantly across conditions.

===Figure 1===

Figure 1 shows the average response rate (percentage of questions answered, averaged across participants) by level of intrusiveness of the questions. Supporting hypothesis (1), the main effect of control was significant ($F(1,130) = 7.71$, $p < 0.001$). Moreover, as one would expect if control specifically influences concern about privacy, the two-way interaction between condition and question intrusiveness was also significant ($F(1,130) = 32.43$, $p < 0.001$): participants with lower control over information release were significantly less willing to answer personal questions, but especially so for more intrusive questions. The average response rate for intrusive questions was 80.8% in Condition 1 and 61.5% in Condition 2 ($t(130) = 4.16$, $p < 0.001$).

STUDY 2

Design

Study 2 was a 2x2 between-subjects design manipulating perceived control and extent of access. It extended Study 1 by adding a between-subjects manipulation of the accessibility of the information provided, thus allowing us to test for hypothesis (2). University students, recruited with the same method adopted for Study 1, answered a shorter version of the same survey. For each of the conditions in Study 1, new conditions were created that increased accessibility by

others: participants read that the website would be accessible by members of the participants' own university *and* the members of another, larger, university in the same neighborhood.

Results

One-hundred and fifty-three subjects participated in Study 2. Supporting hypothesis (1), and replicating the main results from Study 1, the main effect of control was significant ($F(1,155) = 30.65$, $p < 0.001$). As reflected in Figure 2, which compares average response rates in Conditions 2 (uncertain publication of the network profile but smaller accessibility) and 3 (certain publication but larger accessibility), participants with more perceived control over the release of private information show a higher willingness to disclose than participants with less perceived control, even though the former released information to a larger audience (thus exposing themselves to a larger risk of access and usage by others). Moreover, and again consistent with the idea that control specifically influences concern about privacy, there was a significant two-way interaction between condition and question intrusiveness ($F(1,155) = 33.25$, $p < 0.001$). Similarly to Study 1, participants with lower control over information release were significantly less willing to answer personal questions, but especially so for more intrusive questions. On the other hand, and supporting hypothesis (2), the level of authorized accessibility did not affect willingness to disclose significantly ($F(1,155) = 0.196$, $p > 0.10$). The two-way interaction of the accessibility manipulation with question intrusiveness was also not statistically significant.

===Figure 2===

Study 2 supports the central idea that privacy concerns related to accessibility of personal information are trumped by concerns regarding control over release.

STUDY 3

In contrast to Studies 1 and 2, Study 3 tested the impact of providing participants with more, rather than less, control over the release of their information. Study 3 also extended the previous studies by testing the subsidiary hypotheses that (i) the effect of control over information release dominates default effects and *status quo* bias, and (ii) providing granular controls over the release of personal demographic information induces higher disclosure, even though it objectively increases risks of privacy violations (due to the greater potential for identifying a participant whose demographic information is known; see Sweeney, 1997).

Using similar recruitment methods as the previous studies, participants were invited to take a survey on "ethical behaviors." The survey consisted of ten yes/no questions regarding more or less sensitive behaviors, such as stealing, lying, and consuming drugs. Perceived intrusiveness of the questions was established following the same procedure used in Study 1. Study 3 also included a measure of perceived control, enabling a test of whether such perception mediates the effect of the experimental manipulations on willingness to disclose.

Participants read that none of the questions required an answer, and that the researchers intended to publish the results of the study – including participants' anonymous survey answers – in a Research Bulletin. No detail was given as to whom this Bulletin would be accessible, which was a constant feature across all conditions.

Design

The study was a between-subjects design with five conditions.

Condition 1 (no control): participants read that by answering a question they would implicitly give the researchers permission to publish the answer provided. Participants could decide *not* to answer any question, and therefore deny the researchers the ability to publish their answers. In the other conditions, however, such control on publication was made explicit.

Condition 2 (partial control): before answering the ten questions on ethical behaviors, participants were asked to check a box if they agreed to give the researchers permission to publish *all* their answers among the results of the study.

Condition 3 (granular control): for each individual question, participants were asked to check a box, next to the question, to signal that they were willing to grant publication permission of that specific answer. The default option was that the answers would not be published. This condition emulates several Web 2.0 services, such as blogs and online social networks, which provide users with granular control on what to publish online.

Condition 2a: identical to Condition 2, but in addition it asked for permission to publish demographic information (in Conditions 1, 2 and 3, participants read that the demographic information they provided would not be published). Participants could click on separate publication permission boxes for gender, age, and country of birth.

Condition 3a: identical to Condition 3, but the default was that each and every answer provided would have been published.

The survey ended with a set of manipulation checks that allowed us to verify that participants understood how their information would have been used, and a measure of perceived control: on a scale from 1 (No control at all) to 5 (Complete control), we asked how much

participants felt in control on whether their answers would be published among the results of the study.

Results

Main hypothesis. One-hundred and sixty-nine subjects participated in Study 3, of which 33 were assigned to Condition 1, 32 to Condition 2, and 36 to Condition 3 (we discuss the remaining two conditions further below). Supporting hypothesis (1), the main effect of control was significant ($F(2,98) = 49.41$, $p < 0.001$). Figure 3 shows that willingness to disclose increases with the level of control over information publication. In addition, and consistent with the idea that control influences concern about privacy, the two-way interaction between condition and question intrusiveness was significant ($F(2,98) = 18.41$, $p < 0.001$). Participants with lower control over information release were significantly less willing to answer personal questions, but especially so for more intrusive questions. The average response rate for intrusive questions was 44.8% in Condition 1 as compared to 70% and 95.5% in Conditions 2 ($t(67) = -10.58$, $p < 0.001$) and 3 ($t(63) = -3.74$, $p < 0.01$) respectively.

===Figure 3===

We included a measure of perceived control (obtained from the exit-survey) in a mediation analysis (Table 1). We first regressed (Model 1) perceived control on actual control (dummy variables representing Conditions 2 and 3; $F(2,98) = 83.17$, $p < 0.001$), then regressed (Model 2) willingness to disclose information on actual control ($F(2,98) = 44.02$, $p < 0.001$), and finally performed the same regression (Model 3) adding the measure of perceived control ($F(1,$

97) = 3.95, $p < 0.05$). Consistent with standard mediation analysis (which we cannot perform due to the categorical nature of our independent variable), we find that the coefficients on the two dummies for actual control shrink when the mediator is added into the model.[2]

Subsidiary hypotheses. To test for subsidiary hypothesis (i), we first compared response rates and *publication* permission rates from Conditions 3 and 3a (35 participants in the latter condition). We found no statistically significant difference in response rates, but, due to default effects, willingness to publish was significantly higher in Condition 3a (where the default was: publication permitted) ($F(1,69) = 11.126$, $p < 0.01$). Therefore, one may be concerned that subjects' decision to publish personal information was mainly determined by default options, rather than a conscious choice of disclosure. Notice, though, that in Conditions 2 and 3 the default was "publication not permitted," and still most participants (*all* participants in Condition 2 and 72% of participants in Condition 3) *changed* the default option. This indicates that participants were not only willing to provide an answer, but also agreed to its publication. This makes the comparison of response rates across conditions meaningful, since for participants in Condition 1, answering a question implied the publication of the corresponding answer.

Testing for subsidiary hypothesis (ii), a comparison of Conditions 2 and 2a (33 participants in the latter condition) revealed that average response rates did not significantly differ across conditions, but *all* participants in Condition 2a granted permission to publish all three demographic items - which dramatically increases their identifiability (Sweeney, 1997). Remarkably, and consistent with the idea that perceived control decreases people's sensitivity to privacy violations, revealing demographic information voluntarily did not affect their willingness to answer either the mundane or sensitive questions.

[2] We also followed Preacher & Hayes (2008)'s procedure bootstrapping the standard errors for the indirect effects and obtained consistent results.

Discussion

Three experiments provide empirical evidence that perceived control over release plays a critical role in (over)sharing personal information, relative to the objective risks associated with information access and usage by others. In Study 1, people responded to manipulations that decreased control over information release, even though risks associated with information access and use by others were in fact decreased. In Study 2, concerns related to accessibility of private information were trumped by control over release, even though the objective risks associated with revealing sensitive information depend more on the former than the latter. In Study 3, when participants were given explicit control over the release of their personal information, they tended to reveal more, even exposing themselves to higher risks of identifiability.

Our findings can help account for surprising or even contradictory behaviors by users of modern information technologies. For instance, many Facebook users negatively reacted to the introduction of a feature called News Feed, which posted on the user's front page information (such as their recent activities and those of their Facebook "friends") that was *already publicly visible* even before the introduction of this feature (Hoadley et al., 2010; Solove, 2007). The mere perception of control over the release of personal information can sometimes affect individuals more than its actual conditions of access and usage.

Notably, our findings introduce a novel scenario in the scholarly literature on privacy and control. In normative terms, it is conventional wisdom that control over personal information either implies (Culnan, 1993; Elgesem, 1996; Fried, 1984; Lessig, 2002; Miller, 1971; Smith, Milberg, & Burke, 1996; Westin, 1967), or at most does not negatively affect (Laufer & Wolfe, 1977; Tavani & Moor, 2001) privacy protection. However, in positive terms, our results show

that *more* control can sometimes lead to *less* privacy, in the sense of higher objective risks associated with the disclosure of personal information.

The conventional wisdom of privacy as control on personal information flows is so widespread that "control" has become a code-word employed both by legislators and government bodies in proposals for enhanced privacy protection, and by data holders and service providers to deflect criticisms regarding the privacy risks borne by data subjects. For instance, Facebook's CEO Mark Zuckerberg has repeatedly stressed the role of privacy controls as instruments to have "more confidence as you share things on Facebook,"[3] while both Senator Kerry's bill proposal and the Federal Trade Commission's Privacy Report focus on giving users more (privacy) control.[4] In fact, numerous government and corporate entities in the United States have advocated self-regulatory "choice and consent" models of privacy protection that, essentially, rely on users' awareness and control.

The pitch is appealing: users *do* want "more control" over how their information is collected and used (Consumer Reports National Research Center, September 2008, http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html). However, higher levels of control may not always serve the intended goal of enhancing privacy protection. In fact, our findings highlight how technologies that make individuals feel more in control over the release of personal information may carry the unintended consequence of eliciting riskier disclosures.

The paradoxical policy implication of these findings is that the feeling of power conveyed by detailed controls in the privacy settings of several social media, as well as the

[3] "Giving you more control," posted by Mark Zuckerberg on October 10, 2010, available at http://www.facebook.com/blog.php?post=434691727130.
[4] See http://kerry.senate.gov/press/release/?id=223b8aac-0364-4824-abad-274600dffe1c and http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

higher saliency of information release as compared to information access and usage by others, may lower the concerns that people have regarding control over the actual accessibility and usability of that information, driving them to reveal even more sensitive facts about themselves to a larger number of people.

References

Acquisti, A. and Gross, R., 2006, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Proceedings of the Sixth Workshop on Privacy Enhancing Technologies*.

Camerer, C. and Lovallo, 1999, "Overconfidence and Excess Entry: An Experimental Approach," *American Economic Review*, 89(1):306-318.

Culnan, M. J., 1993, "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly*, 17(3): 341-363.

Elgesem, D., 1996, "Privacy, Respect for Persons, and Risk," in *Philosophical Perspectives on Computer-Mediated Communication*, C. Ess ed., New York, State University of New York Press.

Frey, J. H., 1986, "An Experiment With A Confidentiality Reminder In A Telephone Survey," *Public Opinion Quarterly*, 50:267-69.

Fried, C., "Privacy," 1984, in "Philosophical Dimensions of Privacy," F.D. Schoeman (Ed.), New York, Cambridge University Press.

Goodie, A. S., 2005, "The Role of Perceived Control and Overconfidence in Pathological Gambling," *Journal of Gambling Studies*, 21(4):481-502.

Hoadley, C. M., Xu, H., Lee, J. J. and Rosson, M. B., 2010, "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* 9(1):50-60.

Hoffman, D. L., Novak, T. P. and Peralta, M., 1998, "Building Consumer Trust Online," *Communications of the ACM*, 42(4):80-85.

Joinson, A.N., Woodley, A. and Reips, U.D., 2007, "Personalization, Authentication and Self-disclosure in Self-administered Internet Surveys," *Computers in Human Behavior*, 23:275-285.

Klein, G.A., 1998, "Sources of Power: How People Make Decisions," MIT Press, Cambridge, Massachusetts.

Kruger, J., 1999, "Lake Wobegon Be Gone! The 'Below-Average Effect' and the Egocentric Nature of Comparative Ability Judgments," *Journal of Personality and Social Psychology*, 77(2):221-232.

Langer, E. J., 1975, "The Illusion of Control," *Journal of Personality and Social Psychology*, 32(2):311-328.

Laufer, R.S. and Wolfe, R., 1977, "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues*, 33:22-41.

Lessig, L., 2002, "Privacy as Property," *Social Research*, 69(1).

Miller, A. R., 1971, "The Assault on Privacy," Ann Arbor, The University of Michigan.

Moore, D. A. and Healy, P. J., 2008, "The Trouble with Overconfidence," *Psychological Review*, 115(2):502-517.

Petronio, S. S., 2002, "Boundaries of privacy: dialectics of disclosure," SUNY Press.

Phelps, J., Nowak, G. and Ferrell, E., 2000, "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing*, 19(1):27-41.

Preacher, K. J. and Hayes, A. F., 2008, "Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models," *Behavior Research Methods*, 40:879-891.

Singer, E., Hippler, H.J. and Schwarz, N., 1992, "Confidentiality Assurances In Surveys: Reassurance Or Threat?," *International Journal Of Public Opinion Research*, 4:256-68.

Slovic, P., 1975, "Choice between Equally Valued Alternatives," *Journal of Experimental Psychology: Human Perception and Performance*, 1:280-287.

Slovic, P., 1987, "Perception of Risk," *Science*, 236(4799):280-285.

Smith, H. J., Milberg, S. J. and Burke, S. J., 1996, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, 20(2):167-196.

Solove, D.J., 2007, "The future of reputation – gossip, rumor, and privacy on the internet," Yale University Press, New Haven & London.

Sweeney, L., 1997, "Weaving Technology and Policy Together to Maintain Confidentiality," *Journal of Law, Medicine & Ethics*, 25(2&3):98-110.

Tavani, H. T. and Moor, J. H., March 2001, "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies," *Computers and Society*.

Westin, A. R., 1967, "Privacy and Freedom," New York Atheneum.

Weisband, S. and Kiesler, S., 1996, "Self-disclosure on Computer Forms: Meta-analysis and Implications," *Proceedings of the SIGCHI Conference on Human factors in computing systems*, Vancouver, Canada.

Xu, H., 2007, "The Effects of Self-Construal and Perceived Control on Privacy Concerns," *Proceedings of 28th Annual International Conference on Information Systems*, Montréal, Canada.

Figure 1: Average response rate by type of question in Condition 1 (blue, certain publication) and in Condition 2 (red, uncertain publication) – Study 1.

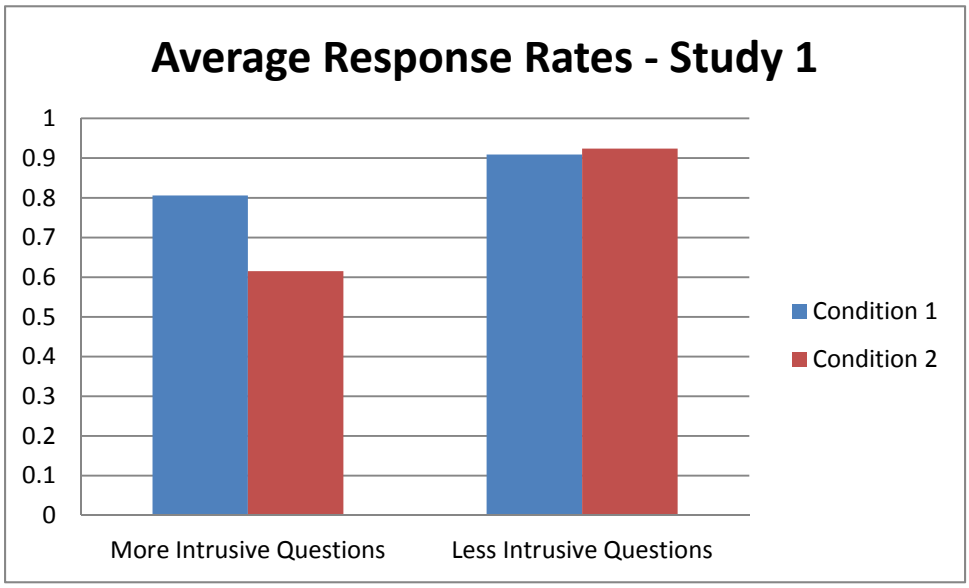

Figure 2: Average response rate by type of question in Condition 2 (red, uncertain publication and smaller accessibility) and in Condition 3 (blue, certain publication and larger accessibility) – Study 2.

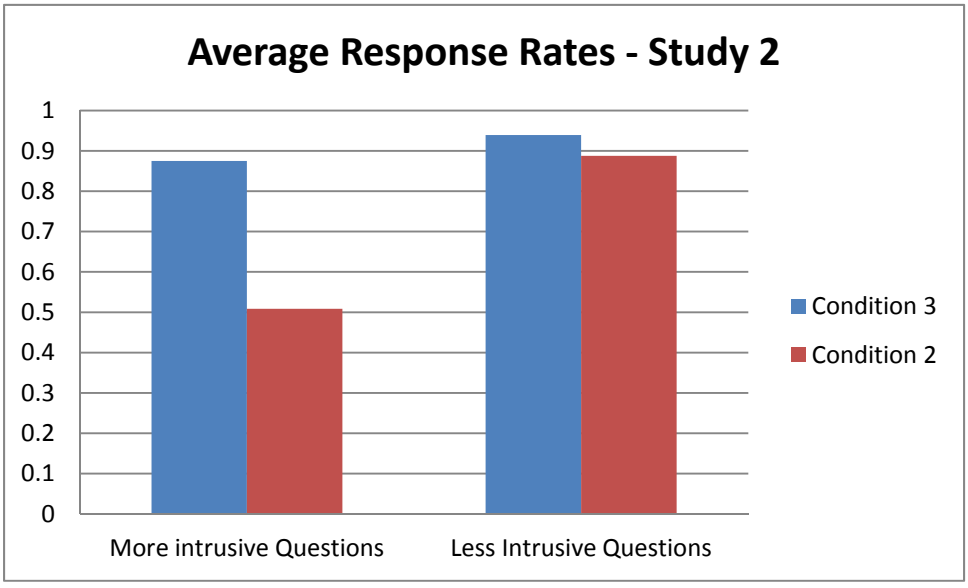

Figure 3: Average response rate by type of question in Condition 1 (red, no control on publication), in Condition 2 (green, partial control) and in Condition 3 (blue, granular control) – Study 3.

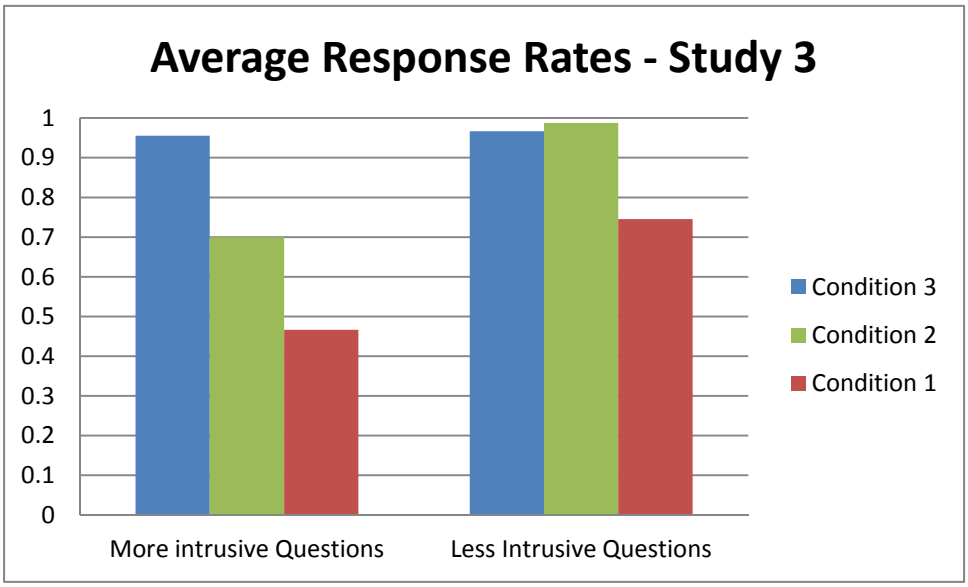

Table 1: Mediation analysis - Study 3. Model 1: Dependent Variable is Perceived Control. Model 2 and Model 3: Dependent Variable is Average Response Rate. Standard errors in brackets. **indicates significance at 5% level. ***indicates significance at 1% level.

	Model 1	*Model 2*	*Model 3*
Perceived Control	-	-	.044**
			(.022)
Condition 2	1.231***	.238***	.183***
	(.177)	(.039)	(.047)
Condition 3	2.217***	.355***	.257***
	(.172)	(.038)	(.062)
Average Response Rate	-	-	-
	N = 101	N = 101	N = 101
	F(2,98) = 83.17	F(2,98) = 44.02	F(3,97) = 31.54