Chapter 1

PRIVACY ATTITUDES AND PRIVACY BEHAVIOR

Losses, Gains, and Hyperbolic Discounting

Alessandro Acquisti
H. John Heinz III School of Public Policy and Management
Carnegie Mellon University
acquisti@andrew.cmu.edu

Jens Grossklags
School of Information Management and Systems
University of California at Berkeley
jensg@sims.berkeley.edu

Abstract Surveys and experiments have uncovered a dichotomy between stated attitudes and actual behavior of individuals facing decisions affecting their privacy and their personal information security. Surveys report that most individuals are concerned about the security of their personal information and are willing to act to protect it. Experiments reveal that very few individuals actually take any action to protect their personal information, even when doing so involves limited costs. In this paper we analyze the causes of this dichotomy. We discuss which economic considerations are likely to affect individual choice and we advance hypotheses about why individuals' information security attitudes seem inconsistent with their behavior.

Keywords: Privacy, Economics, Attitude, Behavior, Immediate Gratification

Preliminary draft. Final version forthcoming in J. Camp and R. Lewis (eds), The Economics of Information Security, Kluwer, 2004

1. Introduction

Several surveys have identified personal information security and privacy as some of the most pressing concerns of those using new information technology. On the Internet, sales for billions of dollars are said to be lost every year because of information security fears.[1] At the same time, several technologies have been made available to protect individuals' personal information and privacy in almost any conceivable scenario - from browsing the Internet to purchasing on- and off-line. With some notable exceptions, very few of these technologies have been successful in the marketplace. There is apparently a demand, and there is an offer. So, why does market clearing seem to be absent?

In this paper we discuss which factors play a role in the decision process of individuals with respect to their privacy and information security concerns, and advance hypotheses about why individuals' information security attitudes seem inconsistent with their behavior.

Understanding this dichotomy is important for the formulation of information policies and for the design of information technologies for personal information security and privacy. Technically efficient technologies have gained only lackluster results in the marketplace. This should be a signal that we need to incorporate more accurate models of users' behavior into the formulation of both policy and technology. In this chapter we try to offer insights on such models. Although in the rest of this chapter we will mostly focus on privacy concerns, most of the analysis can also be applied with minor modifications to personal information security concerns.

2. Personal Information Security and Privacy: Attitudes versus Behavior

Advancements in information technology have often created new opportunities for use and risks for misuse of personal information. Recently, digital technologies and the diffusion of the Internet have have caused both popular concerns and market-based offerings of protective technologies to grow.

Rising concerns have been documented by several surveys and over time. In a Jupiter survey conducted in Spring 1999, forty percent of the 2,403 respondents said that they would have shopped on-line more often if more security of personal information could be guaranteed. A PriceWaterhouseCoopers study in 2000 showed that nearly two thirds of the consumers surveyed abandoned more than once an on-line purchase because of privacy concerns. A Federal Trade Commission (FTC) study reported in 2000 that sixty-seven percent of consumers were "very con-

cerned" about the privacy of the personal information provided on-line (Commission, 2000). A February 2002 Harris Interactive Survey (Harris Interactive, 2002) stated that the three biggest consumer concerns in the area of on-line personal information security were: companies trading personal data without permission, the consequences of insecure transactions, and theft of personal data. According to a Jupiter study in 2002, "$24.5 billion in on-line sales will be lost by 2006 - up from $5.5 billion in 2001. On-line retail sales would be approximately twenty-four percent higher in 2006 if consumers' fears about privacy and security were addressed effectively." (Jupiter Research, 2002).

In addition, some of the numerous surveys in this field not only reveal that individuals are concerned about the privacy and security of their personal information. They also document that certain individuals *claim* they would be willing to take steps to protect their own information - including, in some cases, paying for it.[2]

However, more recent surveys, anecdotal evidence, and experiments have painted a different picture. Chellappa and Sin, 2002, Harn et al., 2002, Spiekermann et al., 2002, and Jupiter Research, 2002 have found evidence that even privacy concerned individuals are willing to trade-off privacy for convenience or to bargain the release of very personal information in exchange of relatively small rewards. In addition, the failure of several online services aimed to provide anonymizing services to Internet users [3] provides indirect anecdotal evidence of the reluctance of most individuals to pay to protect their personal information.

Comparing these apparently conflicting data raises three related questions:

1 Are the two sets of evidence (attitudes revealed in surveys and behavior exposed in experiments) *truly* in contradiction? In other words, is there an actual dichotomy between attitudes and behavior with regard to privacy and security of personal information - or, rather, those apparent discrepancies can be attributed to wrongful measurements and procedures?

2 If a dichotomy actually exists, can we characterize its causes? For example, can we find a relationship between how informed an individual is about privacy and personal information security issues and her attitudes and behavior in this area? What are the relations between her market behavior as an economic agent and her behavior in terms of privacy and information security? What are the psychological factors and economically driving variables that ultimately determine the behavior of information security concerned individuals?

3 Does an observed difference between actual behavior and reported attitudes actually represent a conflict with the economic assumption of rationality and the economic agent's search for an economic optimum? For example, are individuals acting against or in their best interest when they choose *not* to shield themselves from possible information intrusions, or when they accept to give away personal data in exchange for small rewards?

In the rest of this chapter we will comment on questions 1) and 3), but we will focus on question 2). In particular, we will discuss possible heuristics applied by individuals facing privacy and information security-related decisions.

3. Exploring the Dichotomy

The first question to address is whether, in fact, we should be at all surprised by the comparison of results from privacy surveys (such as Commission, 2000) and experiments (such as Spiekermann et al., 2002).

The apparent dichotomy could simply be explained by observing that different people act in different ways, and those who claim that their privacy is important are not those who fail to take actions to protect themselves.

However, that this unlikely is the case should be evident from the magnitudes of the results reported by both experimental and survey data. Although in different setups, the vast majority of subjects (both those interviewed for surveys and those tested during experiments) expressed privacy concerns *and* still traded-off privacy for other advantages (rewards, convenience, etc.). In addition, in their experiment, Spiekermann et al., 2002 controlled for individual behavior and attitudes for each participant. They found that also those individuals classified as privacy advocates would in fact reveal personal information in exchange of small rewards.

Another argument brought forward to refute the existence of a dichotomy relies on the difference between the two following concepts: 1) protecting one's privacy and information security, and 2) offering personal information in exchange of some reward. This argument emphasizes that the markets for protecting and for trading personal information may be related, but not interchangeable.

We agree with the observation that these two markets should not be confused. However, this argument cannot discount the evidence that many privacy-concerned individuals explicitly *claimed*, in surveys, to be willing to pay to protect their privacy - but then acted otherwise. In such case a dichotomy appears *within* the market for information pro-

tection. Furthermore, if the two markets for information protection and information trading are distinct (as well as the decision processes of the individuals in each market), then it remains to be explained where the differences lie and what are their causes. Both protecting and revealing personal information imply material and immaterial (perceived) costs and benefits. Our goal in this chapter is precisely to explore the heuristics through which individuals weight these costs and benefits. it could be that analyzing the differences between the market for information hiding and the market for information sharing, we can also understand better the dichotomy between attitudes towards information hiding and behavior in terms of information sharing.

An additional argument against the existence of a dichotomy is that many individuals may in fact be endorsing a defensive strategy by *not completing* at all certain transactions. Again, many individuals have certainly adopted this strategy to address their privacy concern. Simply observing this, however, does not explain why such approach is also adopted in presence of protective technologies available at low monetary or immaterial costs in the market.

Our analysis instead aims to understanding why individuals decide to take different actions - such as completing a certain transaction without protecting their information, completing the transaction under the umbrella of some technology or policy that protects their information, or not completing the transaction at all. Why privacy concerned individuals can and do react in so many different ways is precisely what we attempt to understand by addressing question 2).

In doing so, we will touch also upon the related question 3): which individual behavior is optimal when her personal information security and privacy are at stake? However, we will only comment briefly on this point. We refer the reader to other (current, e.g., Acquisti, 2002a, and forthcoming) research for more in depth analysis of the existence and efficiency of an equilibrium in the market for personal information.

Attitudes, Behavior, and Privacy

Individuals who claim they are concerned about their personal information act in various, different ways when an information-sensitive situation actually arises. Some complete transactions anyway, without actually protecting personal information. Some give away information for small rewards. Some falsify the information they provide to other parties.[4] Some other avoid information risks altogether by aborting ongoing transactions (and ignoring protecting technologies).

What influences these choices? Are there common, underlying factors which can explain the variety of forms that the attitudes/behavior dichotomy takes? In this section we address this question by analyzing the individual's decision process with regards to privacy issues.

The lack of correspondence between expressed attitudes and subsequent behavior has been detected in several aspects of human behavior and studied in the social psychology literature since LaPiere, 1934 and Corey, 1937. On the other side, evidence of attitudes *causing* a particular behavior has been provided by Ajzen, 1988, Eagly and Chaiken, 1993, and Fazio, 1990; evidence of *behavior influencing attitudes* has been also described by Festinger, 1957, Festinger and Carlsmith, 1959 and Aronson and Mills, 1959. These nuances may make the reader sensitive to the intricacies involved in conducting empirical work on human attitudes and behavior, and aware of the particular challenges involved in interpreting privacy surveys and privacy experiments.

Experimental research work in psychology must always be carefully controlled for other sources of observed differences - in particular those that can be attributed to the research procedures. During interviews or questionnaire sessions, for example, people might feel a pressure to comply to a norm or a need to satisfy the researcher or interviewer; they might report a better version of themselves to avoid embarrassment or to strive for approval. The researcher may influence the results of a study by modifying details in the design: for example, phrasing of questions can induce question-order effect, while in behavioral experiments, the "experimenter effect" may bias participants when they are imposed *surveillance* in a controlled laboratory environment.

Careful research into the attitudes-behavior relationship has highlighted many explaining factors (see, e.g., Fazio, 1990 for a review): *situational* variables (including normative constraints, inducements, and the individual's vested interest in the issue), personality factors (such as self-monitoring, self-consciousness, and the individual's level of moral reasoning), and attitudinal qualities (such as the confidence with which an attitude is held, and the process and time the attitude was formed).

In particular, privacy is a concept interwoven to many aspects of an individual's psychology and personal life, and confronts the individual with many demanding trade-off decisions. Therefore, in our analysis we must expect the existence of several factors affecting the decision process of the individual. As researchers, we are faced with the task to evaluate how those factors are affecting differently the individual at the forecasting (survey) and operative (behavior) phases, thus leading to the variety of adopted privacy strategies quoted above. It may well be that many of the parameters influencing the privacy decision process

of the individual are perceived differently at the forecasting (survey) and operative (behavior) phases, thus leading to the variety of adopted strategies quoted above. The following sections are devoted to discuss those further parameters that we believe add to the understanding of the concept of privacy and the individual decision process in front of information-sensitive decisions.

4. Factors Affecting the Rational Decision Process

Elsewhere, one of the authors (see Acquisti, 2002b) formalizes the abstract economic trade-offs faced by an idealized rational agent who were to decide between information release and information protection. As we move from abstract representations to actual observations, we note that real human beings will face an intricate web of trade-offs dominated by subjective evaluations and uncertainties when attempting to "solve" for the best privacy decision. Because of uncertainties, complexities, and psychological nuances that we describe below, many genuinely privacy sensitive individuals may decide against protecting their own personal information. The decision process considered by an individual therefore does not reduce to (just) an issue of different privacy sensitivities. Several other factors may be playing a role, and their relevance may be realized by the individual only when she is facing an actual decision rather than a fictional survey. The factors that we have observed through surveys, user studies, and analysis that could influence the individual are listed below:

1 Limited information, and, in particular, limited information about benefits and costs.

2 Bounded rationality.

3 Psychological distortions.

4 Ideology and personal attitudes.

5 Market behavior.

If the above factors impact the decision process of the individual, and if their perception during an experiment or survey is different from their perception when an actual decision has to be taken, then these factors may also cause the dichotomy between abstractly stated attitudes and actual behavior. (Of course, the residual dichotomy between attitude and behavior may also be due, as discussed above, to the artificial nature of the survey environment.) Hence we discuss them in more detail below.

Limited information. The amount of information the individual has access to: Is she aware of information security risks and what is her knowledge of the existence of protective technology?

The individual may not be at all aware of information security risks during certain transactions, or may ignore the existence of protective technologies, in which case the consideration of the parameters in an otherwise fully rational model would be distorted.

Gathering full information on every aspect of life is impossible. As a result individuals have to decide based upon incomplete or asymmetric information. Both concepts are well known in the economic literature: asymmetric information was scholarly first analyzed by Akerlof in his famous market for lemons (Akerlof, 1970). Varian discusses similar concepts in the privacy scenario (Varian, 1996). Incomplete information becomes a problem for the individual when she has to commit to an action without a full assessment of the associated privacy-risks. In our scenario, the individual may be ignorant about the risks she incurs by not protecting her personal information or about ways to protect herself. People may assume that institutions and governmental organizations are providing a secure platform for their actions.

Benefits and costs. In particular, information may be limited about benefits and costs related to privacy issues. Obviously, there are several benefits and costs associated to using (or not using) protective technologies. Only some of the costs are monetary (and they could be either fixed - such as adoption costs, or variable - such as usage costs). Other costs may be immaterial: learning costs, switching costs, usability costs, and social stigma when using anonymizing technologies, and may only be discovered through actual usage (see, for example, the difficulties in using privacy and encrypting technologies described in Whitten and Tygar, 1999). A survey participant may not be considering or realizing the existence of all these possible benefits and costs when answering abstract questionnaires.

One example of these hard to assess costs is stigma. Goffman Goffman, 1963 defined stigma as an "attribute that is deeply discrediting" that reduces the bearer "from a whole and usual person to a tainted, discounted one." Consider, for example, the uneasiness of using stronger anonymizing or privacy enhancing technology, like encryption or onion-routing networks, which arises from the fear of judgement of others about what information or practices should be hidden from them. For example, personalized anonymization may be regarded as suspicious by governmental as well as by more community-based organizations. On the other side, *not* using security technologies might represent a psychological cost. For example, an individual might fear embarrassment when requesting

that content filters on a public library computer should be shut down in order to be able to acquire information about topics that overlap with restricted content.

Bounded rationality. Is the individual able to calculate the various parameters relevant to her choice, or is she rather limited by bounded rationality? Is she able to quantify costs and benefits of revealing or hiding information?

Bounded rationality refers to both the inability to calculate probabilities and amounts for risks and related costs for the various possible individual strategies, but also to the inability to process all the uncertain and stochastic information related to information security costs and benefits. Classic economic literature assumes humans to be rational in all aspects of life. However, even in situations with full information humans are not always capable of processing all data and deriving correct conclusions. As one of the first Herbert Simon incorporated constraints on the information-processing capacities of the individuals or entities (see Berger, 1982). Economic theories of bounded rationality can be constructed by modifying classical or perfect rationality assumptions in various ways: (i) by introducing risk and uncertainty into demand and/or cost functions, (ii) by assuming that the entity has only incomplete information about alternatives, or (iii) by assuming complexity in the cost function or other environmental constraints so great as to prevent the actor from calculating the best course of action. The relation to the privacy notion discussed here is obvious. Individuals would collapse under the task of calculating their best strategies to minimize privacy risks for all possible interactions.

In the scenario we consider, when an individual is providing personal information to other parties, she loses control of her personal information. That loss of control propagates and persists for an unpredictable span of time. Hence, the individual is in a position of information asymmetry with respect to the party with whom she is transacting, and the value of the factors to be considered are very difficult to calculate correctly. In other words, the negative utility coming from future potential misuses of somebody's personal information is a random shock whose probability and scope are extremely variable, and the individual is likely in a condition of bounded rationality. For example, a small and apparently innocuous piece of information might become a crucial asset in the right context. Furthermore, an individual who is facing potential privacy intrusions is actually facing risks whose amounts are distributed between zero and possibly large (but mostly uncertain) amounts according to mostly unknown functions. Hence, the individual may not be able to quantify or calculate risks and benefits (see also **?**). In other words,

individuals might decide not to protect themselves because the material and immaterial costs of protection, given the current technologies, are actually higher than the expected losses from privacy intrusions. Thus, the decision not to protect oneself paradoxically may be considered as a rational way to react to these uncertainties: the "discrepancies" between privacy attitudes and privacy behavior may reflect what could at most be called a "rational ignorance."[5]

Psychological distortions. Are the individual's calculations affected by psychological distortions such as self-control problems, hyperbolic discounting, underinsurance? Literature in psychology and behavioral economics has identified numerous factors that can lead to substantial, however, predictable deviations from behavior one would expect from an agent acting according to the classical rational model (see, for example, Rabin and O'Donoghue, 2000).

Individuals might impose constraints on their future behavior even if these constraints limit them in achieving maximum utility. This concept is incorporated into the literature as the self-control problem (sometimes also titled as changing tastes). McIntosh (McIntosh, 1969) tried to approach this puzzling problem in the following way: "The idea of self-control is paradoxical unless it is assumed that the psyche contains more than one energy system, and that these energy systems have some degree of independence from each other." According to this idea, some economists now model individuals as multi-sided personalities, e.g. one personality as a farsighted planner and another one as a myopic doer (Thaler and Shefrin, 1981).

The protection against one's future lack of own willpower could be a crucial aspect in providing a link between information security attitudes and actual behavior. People do want to protect themselves before information losses, but similarly to the attempt to stop smoking or the realization of planned consumption behavior, they might fail. One of the experiments reported in an earlier section of this paper already provided evidence for missing self-control (see, for details, Spiekermann et al., 2002).

Furthermore, evidence of psychological experiments and observations suggest that human discounting is dynamically inconsistent. Ainslie, 1975 found that discount functions are approximately hyperbolic. Hyperbolic discount functions are characterized by a relatively high discount rate over short horizons and a relatively low discount rate over long horizons. This discount structure sets up a conflict between today's preferences, and the preferences that will be held in the future (Laibson, 1997). One can also relax from the assumption of a concrete functional form that is hyperbolic. However, it is generally agreed that

intertemporal preferences take on the following form of time inconsistency: a person's relative preference for well-being at an earlier date over a later date gets stronger as the earlier date gets closer (present-biased preferences) (O'Donoghue and Rabin, 2001).

Thus, individuals tend to under-discount long-term risks and losses while acting in privacy-sensitive situations. Note again the anecdotal finding of Jupiters' survey (Jupiter Research, 2002) that: "82 per-cent of online consumers are willing to provide various forms of information to shopping Websites from which they have yet to make purchases in exchange for something as modest as a 100 USD sweepstakes entry."

This is an interesting phenomenon, which can lead to consumer's exploitation by marketers who can design shopping sites benefitting from the immediate gratification and discounting failures of humans.

A related concept is underinsurance, the situation where an individual or entity has not arranged adequate insurance cover for the financial value of the property insured. Some researchers have already addressed this topic in detail, here also behavioral aspects where discussed. For example, Coate showed that simple altruism can lead to underinsurance by assigned recipients of donations if collective action among donors is only possible before risks are realized (Coate, 1995).

An individual's propensity to underinsure herself against future losses that might incur with low probability but may impose a high risk emerges in the scenario we analyze. Consider, for example, the case of identity theft, where individuals' lack of carefulness can lead (with small probability) to the loss of important personal information like the Social Security Number that can then be used to create a false second identity to impose substantial financial harm on the individual.

Ideology and personal attitudes. Different individuals differ in their sensitivity to privacy. In addition, is the individual considering other ideological factors that affect her attitude towards privacy? For example, does the individual believe that information protection is a right that the government should protect?

People might have the general belief that privacy is an enforced right, which should be guaranteed and not paid for. In this case, the individual is not adopting an utilitarian decision process based on monetary rewards, but is considering a different source of utility and personal satisfaction, based on the advocacy of personal information rights. Hence, this is another possible psychological factor that may affect the behavior of information security-concerned individuals.

Market behavior. Is market behavior (such as propensity to risk, to gains or losses, and to bargaining) affecting her choice?

There may be a relation between the attitudes of a individual with respect to (for example) pricing and bargaining, and her attitude and behavior with respect to information security and privacy. In other words, market behavior may also affect the decision process of individuals who face information related issues. For example, do individuals who bargain a lot also profess more interest in privacy? Are they more or less likely to conform to those attitudes with their behavior?

In particular, let us define a "market-strategic" individual as one that knows that her actions will in turn impact the actions of another party (for example, a merchant) as in a game theoretical setup. So, for example, a strategic individual might refuse a good at a certain price in order to obtain a lesser price in a second offer (see Acquisti and Varian, 2002). A "market-myopic" individual on the other side will not be so forward-looking and will act following short-term interest. Similarly, a "privacy-strategic" individual is one that calculates privacy benefits and risks and acts accordingly; a "privacy-myopic" individual on the other side will be the one who, even if she professes to appreciate privacy, does not take actions to protect herself (because of rational ignorance, as defined above, or because she only considers short-term factors).

5. An Experimental Design

In the previous section we have discussed which factors likely influence the individual's decision process when it comes to privacy issues. Several hypotheses can be advanced to explain individual decision processes. Only an experimental setup under controlled conditions can determine which factors play a dominant role.

While researchers may not able to determine whether the parameters discussed above are perceived differently at the forecasting (survey) and actually operative (behavior) phases, an experimental approach may address related issues:

- Correlate personal information attitudes and behavior to the factors discussed above.
- Isolate the factors that affect the decision process of individuals with respect to their privacy and information security concerns.
- Explain the attitudes/behavior dichotomy through those factors.

So far, in this chapter we have discussed economic aspects of the market for personal information security and privacy. Our analysis was motivated by the observation that many privacy-enhancing technologies are available but few have succeeded in the market. Using economic reasoning we have discussed which factors may affect (and possibly distort) the

decision process of the individual and why privacy attitudes apparently differ from privacy behavior: limited information, self-control problems, other behavioral distortions, bounded rationality.

Our future work aims to provide empirical evidence and experimental results that should enable us to differentiate between the different hypotheses and factors brought forward in this paper and to disentangle the causes of the dichotomy between personal information attitudes and behavior. Such a comparison would require data about the subjects' information security and privacy attitudes and knowledge; data about their market behavior; and data about their actual personal information behavior.

The mixed results met in the marketplace by personal information security technologies is evidence of the need to incorporate more accurate models of user's behavior into the formulation of policy and technology guidelines. We hope that our ongoing analysis can be useful to the design of information policies and information technologies.

Notes

1. See, for example, Commission, 2000.
2. See Truste-Boston Consulting Group 1997 privacy survey, quoted by the Center for Democracy and Technology, www.cdt.org.
3. See Brunk, 2002.
4. See the 8th annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, www.gvu.gatech.edu.
5. See, in a different context, Lemley, 2000.

References

Acquisti, Alessandro (2002a). Privacy and security of personal information: Economic incentives and technological solutions. In *1st SIMS Workshop on Economics and Information Security.*

Acquisti, Alessandro (2002b). Protecting privacy with economics: Economic incentives for preventive technologies in ubiquitous computing environments. In *Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing - UBICOMP '02.*

Acquisti, Alessandro and Varian, Hal R. (2002). Conditioning prices on purchase history. Technical report, University of California, Berkeley. First draft: 2001. Presented at the European Economic Association Conference, Venice, IT, August 2002.

Ainslie, George W. (1975). Specious reward: A behavioral theory of impulsiveness and impulsive control. *Psychological Bulletin*, 82:463–496.

Ajzen, Icek (1988). *Attitudes, personality, and behavior*, chapter 6. Open University Press, Milton-Keynes, England.

Akerlof, George A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84:488–500.

Aronson, Elliot and Mills, Judson (1959). The effect of severity of initiation on the devaluation of forbidden behavior. *Journal of Abnormal and Social Psychology*, 59:177–181.

Berger, Peter L. (1982). *Models of bounded rationality, Vol. I-III*. The MIT Press, Cambridge, MA.

Brunk, Benjamin D. (2002). Understanding the privacy space. *First Monday*, 7. `"http://firstmonday.org/issues/issue7_10/brunk/index.html`.

Chellappa, Ramnath K. and Sin, Raymong (2002). Personalization versus privacy: An empirical examination of the online consumer's dilemma. In *2002 Informs Meeting*.

Coate, Stephen (1995). Altruism, the samaritan's dilemna, and government transfer policy. *American Economic Review*, 85(1):46–57.

Commission, Federal Trade (2000). Privacy online: Fair information practices in the electronic marketplace. `http://www.ftc.gov/reports/privacy2000/privacy2000.pdf`.

Corey, S.M. (1937). Professional attitudes and actual behavior. *Journal of educational psychology*, 28(1):271 – 280.

Eagly, Alice H. and Chaiken, Shelly (1993). *The Psychology of Attitudes*, chapter 4. Harcourt Brace Jovanovich College Publishers, Fort Worth, TX.

Fazio, Russell H. (1990). Multiple processes by which attitudes guide behavior: The mode model as an integrative framework. *Advances in experimental social psychology*, 23:75–109.

Festinger, Leon (1957). *A theory of cognitive dissonance*. Row Peterson, Evanston, IL.

Festinger, Leon and Carlsmith, James M. (1959). Cognitive consequences of forced compliance. *Journal of Abnormal and Social Psychology*, 58:203–210.

Goffman, Erving (1963). *Stigma: Notes on the Management of Spoiled Identity*. Prentice-Hall, Englewood Cliffs, NJ.

Harn, Il-Horn, Hui, Kai-Lung, Lee, Tom S., and Png, Ivan P. L. (2002). Online information privacy: Measuring the cost-benefit trade-off. In *23rd International Conference on Information Systems*.

Harris Interactive (2002). First major post-9-11 privacy survey finds consumers demanding companies do more to protect privacy; public wants company privacy policies to be independently verified. `http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429`.

Jupiter Research (2002). Seventy percent of US consumers worry about online privacy, but few take protective action. `http://www.jmm.com/xp/jmm/press/2002/pr_060302.xml`.

Laibson, David (1997). Golden eggs and hyperbolic discounting. *Quarterly Journal of Economics*, 62(2):443–477.

LaPiere, Robert (1934). Attitudes versus actions. *Social Forces*, 13:230–237.

Lemley, Mark (2000). Rational ignorance at the patent office. Technical report, Berkeley Olin Program in Law and Economics, Working Paper Series.

McIntosh, Donald (1969). *The Foundations of Human Society*. The University of Chicago Press, Chicago, IL.

O'Donoghue, Ted and Rabin, Matthew (2001). Choice and procrastination. *Quarterly Journal of Economics*, 116(1):121–160.

Rabin, Matthew and O'Donoghue, Ted (2000). The economics of immediate gratification. *Journal of Behavioral Decision Making*, 13(2):233–250.

Spiekermann, Sarah, Grossklags, Jens, and Berendt, Bettina (2002). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *3rd ACM Conference on Electronic Commerce - EC '01*, pages 38–47.

Thaler, Richard and Shefrin, Hersh M. (1981). An economic theory of self-control. *The Journal of Political Economy*, 89:392–406.

Varian, Hal R. (1996). Economic aspects of personal privacy. In *Privacy and Self-Regulation in the Information Age*. National Telecommunications and Information Administration.

Whitten, Alma and Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium*. `citeseer.nj.nec.com/whitten99why.html`.