TRUST, ETHICS, AND PRIVACY

IAN GOLDBERG, AUSTIN HILL, ADAM SHOSTACK*

INTRODUCTION 000
I. TRUST AND RELIANCE 000
A. *Why People Don't Rely on Policies* 000
B. *Trust Online* 000
C. *"For Your Own Good"* 000
D. *The Public Good* 000
II. ETHICS AND PRIVACY 000
III. DESIGN IS NOT NEUTRAL 000
A. *Toll Roads* 000
B. *Frequent-Buyer Cards* 000
C. *Amazon.com* 000
CONCLUSION

INTRODUCTION

In our increasingly electronic world, privacy has emerged as an extremely important issue. As more and more people and businesses communicate and transact on the Internet, concern has grown over what "going online" means to privacy. It is clear that something must be done to protect privacy in the electronic age, but that in turn produces another concern—*who* should make those decisions about our online privacy and how should those decisions be made?

Some commentators suggest that this loss of privacy through technology is inevitable.[1] Others argue that various forms of regulation will solve the privacy problem.[2] We propose that privacy is a matter best addressed by ethically

* Zero Knowledge Systems, Inc. Email: Iang, Austin, & Adam@zeroknowledge.com

[1] *See, e.g.*, A. Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?* 52 STAN. L. REV. 1461, 1462 (2000) (quoting Scott McNealy, the CEO of Sun Microsystems as saying "You have zero privacy. Get over it."); *see also* DAVID BRIN, THE TRANSPARENT SOCIETY 5 (1998) (exemplifying the notion that technology infringing on privacy is "here to stay"); Edward C. Baig, Marcia Stepanek & Neil Gross, *Privacy: The Internet Wants Your Personal Info. What's in It for You?*, BUS. WK., Apr. 5, 1999, at 84 (discussing the prevalence of McNealy's "get over it" attitude).

[2] *See, e.g.*, Mark E. Budnitz, *Privacy Protection For Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847, 848 (1998) (arguing that statutory protection is necessary to protect privacy); Froomkin, *supra* note 1, at 1542; Baig et al., *supra* note 1, at 84 (noting that privacy advocates have inspired politicians to introduce scores of privacy legislation at both the state and federal level, and that a few

motivated design choices, and that applying ethical principles is the only effective way to build trust online.

In this paper we examine the relationships between trust and reliance, as well as how they relate to ethics and privacy. We begin by discussing the various meanings and interpretations of trust, and why achieving trust is a goal. We look at differences between trust and reliance, and why each can be challenging to achieve. We examine both offline and online scenarios, and examine how they differ. We look at the ways that broad based trust online is damaged by the behavior of some individuals and groups. From there, we discuss whether it is possible to build trust by demonstrating ethical behavior and, if so, whether privacy is part of that ethical behavior. Finally, we examine three systems and look at the interaction between design, privacy, and trust.

I. TRUST AND RELIANCE

A great many individuals, groups and companies invest time and energy into building trust. For example, the Virginia Education Association trumpets that "Teachers [are the] Most Trusted People in America," and RSA Security refers to itself as "The Most Trusted Name in e-Security."[3] While the motives that individuals, groups, and companies have for declaring themselves "most trusted" clearly vary, what is less obvious is that their conception of what trust is varies a great deal as well.

One conception of trust is the implicit claim that the most widely used are the most trusted. This is particularly true of businesses who build around the old salesman's promise, "No one ever got fired for buying IBM."[4] Conceptions of, and requirements for trust are dependant on context. While you might trust someone to fix your car, you probably would not trust him or

advocate tight governmental controls on personal information resembling Europe's safeguards promulgated in Fall of 1998); Naturally, e-businesses are concerned that government regulation will increase their operating costs, and have therefore begun to regulate themselves. *See* WILLIAM J. CLINTON & ALBERT GORE, JR., FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 13 (1997) ("The Administration supports private sector efforts now underway to implement self-regulatory privacy regimes."); Baig et al., *supra* note 1 at 84-85.

[3] *See Teachers Most Trusted in America*, VIRGINIA JOURNAL OF EDUCATION (Jan. 1999) (listing members of the teaching profession as the most trusted people in America); *RSA Security's homepage*, (visited February 5, 2001) <http://www.rsasecurity.com>. Interestingly, when we searched "most trusted" on Google.com, a web search engine akin to Yahoo, Lycos or Alta Vista, most of the top twenty results were for gambling sites, escort services, and politicians. We leave the discussion of why this may be for another day, and wish only to note now the difficulty of receiving compensation for poor service from any of the three. We note also that Google is well regarded by the technical community for using clever tricks, such as returning websites containing the inputted search criteria like "most trusted" in order of the websites' overall popularity.

[4] *See Brands Need More Attention*, ADVERTISING AGE, July 4, 1994, at 8 (noting truism to show how trustworthy the brand name IBM used to be).

her to be responsible for your child's education. Therefore, the degree of need for trust, and the type of trust needed are dependant on the situation. Organizations such as the teacher's association need to reinforce the trust that people place in them because such trust is required before anyone will place a child in their care. An entirely different sense of the word is captured in Amazon.com's privacy policy: "Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly."[5]

For most information, choosing to trust an organization with personal information is probably not as important a decision as choosing to trust someone to educate your child.[6] Even so, while you probably would not hand over all decision-making power to your child's educator, you do repose such trust in Amazon.com, who now has total control over the use of the information you have given them. We suggest that in all of these contexts reliance is a better term than trust.

Reliance, in non-legal parlance, is "the act of relying, or the condition or quality of being reliant; dependence; confidence; trust; repose of mind upon what is deemed sufficient support or authority."[7] Of particular interest are the last few words of this definition. Reliance is built on a rational assessment of risks and justifications. Reliance can be built, either over time or quickly, on a variety of foundations that justify the choice to rely. One such foundation is the ability to fall back on a legal or similarly authoritative system if reliance proves to have been misplaced. Another justifying foundation is the belief that a business's longevity is directly proportional to its reliability. Businesses advertise having been around for a long time as a way of saying, "We're reliable, people keep coming back with their business." In contrast to reliance, trust refers to those situations where someone acts as if those justifying foundations exist, without knowing whether or not that is true.

In discussing the difference between trust and reliance, Schelling points out that the question to ask was never "Can we trust the Russians," but "Can we rely on the Russians to act in their own rational self-interest?"[8] This difference is important. Reliance can be built around authority, and mutually suspicious organizations can rely on one another, or upon mutually agreeable third parties.

Building the structures on which reliance rests takes time and energy. Even when those structures already exist in a meaningful way, verifying that they are

---

[5] *Amazon.com Privacy Notice* (visited January 30, 2001) <http://www.amazon.com/exec/obidos/tg/browse/-/468496/103-9093305-0522210>.

[6] An example of highly sensitive information might be HIV test results.

[7] Reliance: 1. The act of relying; 2. The condition or attitude of one who relies: dependence, confidence; 3. Something or someone relied upon: mainstay. MERRIAM-WEBSTER'S 3RD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE 1917 (3d ed. 1986).

[8] *See* Thomas Schelling, Address at the Boston University Trust Relationships Conference (Sep. 23, 2000).

in place and effective has a cost. For example, a cross-border transaction may have to consider two or more countries' laws. In the event of a dispute, the law governing the underlying transaction may differ from the law in the country where the defendant's assets are located. To determine whether the transaction can be enforced, a lawyer must carefully analyze the law in both countries. Knowing which country's law will prevail can have a profound effect on the terms of the deal. While traditionally this has been a concern only for companies engaged in business in several countries, the Internet brings this problem to everyone.

Many of the ordinary cues that physical interaction with businesses provides do not exist when dealing with an online organization. The fact that a website is based in another country has no effect on how long it takes to load, or any other aspect of how easy it is to use. Things that are obvious in the physical world can become invisible on the Internet, making it harder for users to assess whether a web-based organization is reliable. This makes it harder for the user to rely on the website to do the "right thing."

Another distinction between the online and offline world is that it is harder to create a "false front" offline.[9] With a small investment of time and money, it is reasonably easy to create what only appears to be a large, well-stocked online bookstore. Because the physical cues that something is real do not exist online, it is easier to believe that something is fake, or misleading.[10] In addition, the lack of physical cues limits the credibility of the privacy policies and self-regulation that many American businesses promote.[11]

---

[9] *See* Peter Steiner, *Cartoon*, NEW YORKER, July 5, 1993, at 61 (depicting an oft-quoted cartoon with the caption, "On the Internet, nobody knows you're a dog."); *see also* Helen Nissenbaum, *Securing Trust Online: Wise Choice or Contradiction*, *in* VIRTUAL PUBLICS: POLICY AND COMMUNITY IN AN ELECTRONIC AGE (Beth Kolko ed., 2000) (describing the difficulty of faking personal information "offline"); *Cf.* Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. CHI. LEGAL F. 77, 78 (1996) (noting that the aspects of behavior a person chooses to reveal are governed in part by the person's expectations about whether knowledge of those actions may be used to actor's detriment).

[10] *See* Nissenbaum, *supra* note 9.

[11] In fact, website privacy policies do not deserve much credibility, as relatively few websites are taking the steps advocated by the FTC since 1998. These steps are known as the "Fair Information Practice Principles." For the original code of Fair Information Practice Principles, see DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973); *see also* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE II (2000) [hereinafter FTC REPORT] (finding that only twenty percent of surveyed websites collecting personal information employed, at least partially, all of the fair information practice principles set by the FTC); GEORGETOWN INTERNET PRIVACY POLICY SURVEY: REPORT TO THE FEDERAL TRADE COMMISSION 6 (1999) (hereinafter GIPP REPORT) (finding that only 13.6% of surveyed websites contained at least one of the elements of fair information guidelines set forth by the FTC).

B. *Why People Don't Rely on Policies*

Many have suggested that privacy policies are a basis for self-regulation.[12] Those policies are supposed to do a number of things, including to reassure customers that their privacy is respected, to ensure compliance with relevant laws, and to avoid the addition of new laws.[13] Privacy policies could be an effective tool for managing assurance and reliance, especially if a trustworthy agent certifies those policies as authentic.[14] The use of agents to authenticate online service providers is known as a "seal program."[15] Unfortunately, since the certified pay the certifiers there is a risk of regulatory capture.[16] It appears that consumers understand this risk, as no seal program has established substantial customer reliance (dare we say trust?) to date.[17]

---

[12] *See, e.g.*, CLINTON & GORE, *supra* note 2, at 12-13 (advocating disclosure through practices like privacy policies as essential practice to ensure privacy); NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION, ELEMENTS OF EFFECTIVE SELF-REGULATION FOR PROTECTION OF PRIVACY (1998) (Discussion Draft) (visited February 4, 2001) <http://www.ntia.doc.gov/reports/privacydraft/198dftprin.htm> (outlining principles of fair information practices and specifying the use of privacy policies in implementing them). *But see* Froomkin, *supra* note 1, at 1542 (arguing that only a mix of self-regulation, law, and technological design principles will suffice to ensure privacy on the Internet); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 771 (1999) ("[T]he theory of self-regulation has normative flaws and that public experience shows the failure of industry to implement fair information practices.").

[13] *See* CLINTON & GORE, *supra* note 2, at 12-13.

[14] *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 114 (1996) (arguing that trusted third parties in electronic transactions may become essential (but not sufficient) to creating trust online for most electronic commerce).

[15] WEB SEALS: A REVIEW OF ONLINE PRIVACY PROGRAMS, 22D INT'L CONF. ON PRIVACY AND PERSONAL DATA PROTECTION i (2000).

[16] The concept of regulatory capture was introduced in 1952 by Samuel Huntington. It refers to the tendency of regulators to show a preference for the desires of those regulated over the needs of the public. The term is widely used by those who study the effects of administrative agency regulation. *See generally* Samuel P. Huntington, *The Marasmus of the ICC: The Commission, the Railroads, and the Public Interest*, 61 YALE L.J. 467 (1952) (describing the effects of railroad lobbying on the Interstate Commerce Commission); George J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. OF ECON. & MAN. SCI. 3 (1971) (setting forth the theory of regulatory capture); Sam Peltzman, *Toward a More General Theory of Regulation*, 19 J.L. & ECON. 211 (1976) (formalizing an economic theory of regulatory capture).

[17] *See* FTC REPORT, *supra* note 11, at 6-7 ("Despite the fact that□□□[seal programs] have experienced continued growth, the impact of online privacy seal programs on the Web remains limited□□□□'); *see also* CHESKIN RESEARCH & STUDIO ARCHETYPE/SAPIENT, ECOMMERCE TRUST STUDY 16 (1999), available at: <http://www.studioarchetype.com/cheskin/assets/images/etrust.pdf> (summarizing data of survey results, and finding that the most familiar seal was VeriSign at 36% recognition, and that only 53% of those familiar with it would trust a VeriSign site more). *But see* Lorrie

The willingness of consumers to rely on privacy policies is partially dependent on the cost of relying on and verifying those policies. Many privacy policies require the consumer to recognize changes to those policies. In addition, consumers tend to visit a large number of web sites, each with a unique privacy policy.[18] Both the number of different privacy policies and the potential for change at any time in these policies drive up the cost of reliance substantially. The privacy policy author could, with little effort and expense, assume the cost of notifying interested consumers about changes to the policy. Still, that has not happened, and even simple steps like posting a last-changed date or a version number are rarely taken. That the policy author has pushed this cost to the consumer, whose investment will be significantly greater, indicates an almost inexplicable disrespect for people.[19] This investment would show that the company is interested in helping people understand its privacy policies, which might increase business.[20] When the benefit to a consumer is sufficiently high, the consumer may be willing to accept the cost of relying on and understanding these privacy policies. When the benefits are not sufficiently high, however, this burden is an inducement to go elsewhere.

Consumer reliance is further weakened by failures in online security systems. The nearly continual reports of such failures with respect to web sites,[21] online vendors,[22] and software vendors[23] all contribute to a general sense that information security is a difficult problem and that relying on an

Faith Cranor, Joseph Reagle, & Mark S. Ackerman, *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, *AT&T Labs-Research Technical Rep. TR* 99.4.3 (1999) (visited 2001) <http://research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm> (finding that "a joint program of privacy policies and privacy seals seemingly provides a comparable level of user confidence as that provided by privacy laws").

[18] One survey reports that as of July 2000, there are more than 93 million unique Internet hosts. *See Internet Software Consortium Internet Domain Survey* (visited February 10, 2001) <http://www.isc.org>.

[19] Unless, of course, there is a vested interest in making it easy for consumers to ignore privacy policies.

[20] "One study estimates that privacy concerns may have resulted in as much as $2.8 billion in lost retail sales in 1999, while another suggests potential losses of up to $18 billion by 2002 (compared to a projected total of $40 billion in online sales), if nothing is done to allay consumer concerns." FTC REPORT, *supra* note 11, at 2.

[21] Website defacements occur at a rate of more than 25 per day, and are now automatically archived and analyzed at sites such as Attrition.org. *See Attrition Annual, Monthly Counts, Defacement Day Tables and Chart, 1995 to Present* (visited February 2, 2001) <http://www.attrition.org/mirror/attrition/annuals.html>.

[22] *See, e.g.*, *Hacker Takes Credit-Card Numbers*, WASH. POST, Jan. 11, 2000, at E02 (reporting hacker's misappropriation of up to 300,000 credit card numbers from CD Universe, and subsequent publication of up to 25,000 of them on a web site).

[23] *See, e.g.*, Sara Robinson, *Microsoft Shuts Security Breach in E-Mail System*, N.Y. TIMES, Aug. 31, 1999, at C1 (describing the hacker attack on Microsoft's free e-mail service, Hotmail, that exposed the e-mail accounts of tens of millions of subscribers).

unknown party to get it right may be unwise. Security failures are one example of a more general set of concerns surrounding the reliability of the Internet. While this may seem tautological, the concept of reliance requires reliability.

The combination of regulatory capture, asymmetrical cost allocations, and reliability concerns all combine to make reliance hard to achieve in an Internet context. Given the ongoing difficulties in establishing reliance online, many companies are trying to build reliance or trust in alternate ways. Some companies and governments are attempting to build reliance through new laws. We will not, however, examine these reliance measures, but instead turn our attention to trust.

B. *Trust Online*

Trust is based on an assured belief that another person displays integrity, veracity, justice, and other aspects of ethical behavior, and will continue to do so. Building up trust requires an investment of time and energy.[24] It may also require that the person who wishes to be trusted make himself vulnerable in some way. This need for vulnerability is related to standard iterated prisoners' dilemmas.[25] By choosing to act in a tit-for-tat fashion, and starting with a cooperation action, the actor signals that he is are "trustworthy."[26] The actor chooses to be vulnerable in order to signal that he understands the implications of a game that is played for countless iterations.[27] In game theory, a lack of

[24] *See* TAMAR FRANKEL, TRUSTING AND NON-TRUSTING: COMPARING BENEFITS, COST AND RISK, BOSTON UNIVERSITY SCHOOL OF LAW WORKING PAPER 99-12 14 (1999) (describing the costs of establishing personal trusting relationships).

[25] In a simple prisoners' dilemma game where the game is played only once, both players rationally choose the least efficient equilibrium, because neither knows how the other prisoner will choose. *See* ROGER B. MYERSON, GAME THEORY: ANALYSIS OF CONFLICT 97-98 (1991). Standard iterated games are those in which there are an infinite (or what the players believe is probably infinite) number of iterations of the game, and the players always have "standard information"—they always have complete knowledge of the historical behavior of the other player. *See id.* at 308-31 (describing standard repeated games, including standard repeated prisoners' dilemmas).

[26] A tit-for-tat strategy involves choosing the same move as the opponent chose in the previous iteration. Thus, if players employ a tit-for-tat strategy and begin with a cooperative move, they can avoid the result of the simple prisoners' dilemma and achieve optimal equilibrium. *See id.* at 325. For a good example of this strategy in trust terms, see Oliver E. Williamson, *Calculativeness, Trust, and Economic Organization*, 36 J.L. & ECON. 453, 466 (1993):

> Say for example, X tells Y, "I will begin by trusting you, hoping that you will honor that trust. Indeed, I will continue to trust you as long as you do not abuse that trust. But if ever you abuse that trust, I will never again trust you. If Y hears and believes that statement, and if the game is played repeatedly (with high probability) then the honor-trust arrangement is self-enforcing.

[27] With an unknown number of iterations, a player must always consider the effect of his or her choice on the future moves of the other player. *See* MYERSON, *supra* note 25, at 308.

knowledge of when interaction will end ensures that players do not defect in the last round.[28] This behavior is very similar to that of reliance, but here it occurs where players do not have recourse to an outside authority.[29] Vulnerability must be present in order to allow the "defection" behavior. If someone cannot harm you in an interaction, you gain no information about what they might do in a situation where they can. Therefore, the repeated presence of vulnerability produces more information about someone's behavior and enables an individual to trust that the other party will behave in a mutually beneficial fashion.[30]

In addition to trusting individuals, consumers are capable of trusting organizations. This trust is usually based on an organization's long-standing, trumpeted commitment to some value that the person holds dear. The vulnerability may not be explicitly acknowledged, but the organization's fund raising and membership activities indicate whether it will act as a trustworthy representative. This is the aim of organizations ranging from Amnesty International to the National Rifle Association, both of whom make an effort to build themselves up as trusted emissaries of their interest groups. Similarly, businesses such as Ben & Jerry's and The Body Shop have used their advocacy of causes to build brand and customer loyalty.[31] Although building trust does

Choosing a cooperative move in the beginning—the irrational choice in a simple prisoners' dilemma—would thus signal the desire to achieve optimal equilibrium in the subsequent iterations, but of course makes the player very vulnerable to defection by the other.

[28] Repeated games in which the players know when the interaction will end are called finitely repeated games; in "striking contrast" to infinitely repeated games, the "unique equilibrium" of finitely repeated games, like the simple form, "is for both players to always play selfishly." *See* MYERSON, *supra* note 25, at 337.

[29] Since there is no third party, there are only two options: go ahead and exchange, and hope for the best (which may or may not result in an optimally efficient game), or decide to walk away (which would definitely be inefficient, although, not the least efficient). A third party/authority provides a safeguard, because the third party would know if one of the players played selfishly. So a player has further incentive to choose cooperatively. *See* Williamson, *supra* note 26, at 467 ("Competition provides a safeguard.").

[30] Of course, it can also create a situation in which both players "mutually punish" each other for the rest of the game; this is obviously suboptimal. *See* MYERSON, *supra* note 25, at 328. A modified tit-for-tat strategy, called "getting even," avoids this suboptimal spiral while maintaining the benefit of vulnerability by restricting retaliatory behavior to "justified responses." For example, if one player chooses a selfish move, the other player retaliates with a selfish move in the next game, but the first player should assume the response was justified and not respond with counter-retaliatory move. Thus, the game can eventually return to an optimal equilibrium. *See id.* at 326-27.

[31] *See* Thomas W. Dunfee, *Corporate Governance in a Market with Morality*, 62 LAW & CONTEMP. PROBS. 129, 141 (1999) ("Firms such as the Body Shop, Tom's of Maine, and Ben & Jerry's target the moral desires of potential customers by engaging in social-cause marketing. Such firms seeks to identify with particular social causes, such as saving whales, as a means of attracting consumers who want to support those causes. Consumers may choose to do business with them solely on the basis of an assumed alignment of moral

not require every online entity to go so far as to engage in cause marketing, building trust does require every online entity to address security and privacy.

Nearly every site now has a privacy policy, and most start with the words "Your privacy is important to us."[32] Consumers, however, evaluate this promise in light of many factors. One of those factors is the visible investment in privacy that a company makes, ranging from the obvious, like the use of seal programs, to the less obvious, like the type of information the site is collecting, and how that information is used.[33] These cues may not be consciously examined or analyzed, but consumers continue to show a great reluctance to offer their personal information online because they neither trust, nor are willing to rely on, the promises made.

Investment in privacy resembles an investment in brand[34]- it is a method of signaling concern for the things that concern the consumer and demonstrating that the investor plans to be around for a while.[35] While each of these may engender trust, however, that trust is not immune to erosion. We proceed by examining the behaviors that can lead to an erosion of trust.

C. *"For Your Own Good"*

Many systemic privacy invasions are justified as in the interest of the subject of the invasion.[36] If this justification is in fact sufficient, there is no

---

preferences.").

[32] There are literally thousands of websites with those exact words, and thousands upon thousands more with a variation of them. *See, e.g.*, *InvesTools.com* (visited February 4, 2001) <http://www.investools.com/cgi-bin/IT/boilerplate/privacy> ("It is our intent to build a long-term relationship with you based on trust, and as your trusted source for investment advice we cannot afford to break that bond with you at any time."); *Funeralvalue.com* (visited February 4, 2001) <http://www.funeralvalue.com/privacy.html>; *Webcommend.com* (visited February 4, 2001) <http://www.webcommend.com/privacy.html>.

[33] The Center for Democracy and Technology's Guide to Online Privacy advises consumers to scrutinize a site's privacy policies with specific questions about the collection and use of information about the visitor. *See* Center for Democracy and Technology, *CDT's Guide to Online Privacy* (visited February 4, 2001) <http://www.cdt.org/privacy/guide/start/privpolicy.html>; *see also* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7-14 (1998) (outlining fair information practice guidelines designed to allow companies to address consumer concerns about privacy).

[34] *See* Baig et al., *supra* note 1, at 87. It is also possible to invest in privacy in a way that is closer to malpractice insurance. This happens when information about privacy investment is not communicated to customers.

[35] *See, e.g.*, Tulin Erdem & Joffre Swait, *Brand Equity As a Signaling Phenomenon*, 7 J. CONSUMER PSYCHOL. 131 (1998) (showing that consumers will use brand name as a signal of a product's quality in asymmetrical information situations

[36] For a critical examination of various justifications in the business interest context, see Gandy, *supra* note 9, at 80-101.

reason to reject the Fair Information Practice guidelines.[37] After all, the subject will then agree to the collection of personal data, the data will be used for its primary purpose, and the subject will be given a chance to agree to secondary use. It is when the data collectors make decisions "on behalf of" the subject that we encounter a problem of moral hazard.[38] There is a conflict of interest between the data collector who wants the information for a particular use and the subject whom he fears will not consent. Thus, there is a hazard that the data collector is not acting "on behalf" or "in the best interests" of the subject. Obviously, once detected, such behavior will undermine trust.

D. *The Public Good*

A similar risk of erosion exists when privacy is subsumed to "the public good," although this depends on how deeply the affected people feel about privacy. Public health officials often infringe on individual privacy "for the public good."[39] For example, many states have created, by statute, tumor registries that track information about every diagnosis of cancer.[40] In New York, all cancers are reported to the state department of public health in a fully identified form, so that the state can perform epidemiology. Employees of the Department of Public Health have in the past sent cards to a cancer patient's friends and family, not realizing that the cancer was being kept secret. Regardless of the wisdom in keeping cancer a secret, it is destructive to the trust relationship that must exist between a patient and his doctor.[41] Further,

---

[37] *See* RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, *supra* note 11; (outlining fair information practice guidelines); *see also* discussion *infra* Section III.

[38] *See* Tom Baker, *On the Genealogy of Moral Hazard*, 75 TEX. L. REV. 237, 239 (1996) ("In the economics literature and in the law and policy debate that draws upon this literature, 'moral hazard' refers to the tendency for insurance against loss to reduce incentives to prevent or minimize the cost of loss.").

[39] "Every state requires health care providers to report selected identifiable patient information to state agencies. Reportable information may include communicable diseases, violent injuries (*e.g.*, gunshot wounds), occupational diseases or injuries, epilepsy, congenital defects, and injuries from child abuse or neglect. In addition, an increasing number of states require the reporting of information relating to abortions, certain prescription drugs, cancer, and battered adults. The number of reportable medical conditions has increased in recent years." Robert M. Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 N.C. L. REV. 255, 274 (1984) (discussing the impact of availability of increasingly detailed medical records and the growing need for them).

[40] *See, e.g.*, N.Y. COMP. CODES R. & REGS. tit. 10, § 1.31 (2001). In all there are 39 states with cancer registries. *See* CENTERS FOR DISEASE CONTROL AND PREVENTION, CANCER REGISTRIES: THE FOUNDATION FOR COMPREHENSIVE CANCER CONTROL 1 (2000) (showing a map of states with cancer registries).

[41] Doctors need trust, not reliance, because they need information in an unfiltered form. If there is no trust, the patient will filter the information that he gives to his doctor. This nominally rational behavior is only actually rational if the patient knows enough to judge

when there is no trust and no respect for medical privacy, people may choose not to seek medical care.[42] Even if the individual does seek medical care, he may choose to do so elsewhere, putting the psychic value of privacy above the value of local health care. In game theoretic terms, these trust eroding behaviors are acts of defection by the organization that performs them. Worse, these behaviors may signal an intent to defect again in the future.

II. ETHICS AND PRIVACY

To build a relationship of trust, there must be an assurance that the other player will act in a predictable manner. We now examine the role of ethics and privacy in that signaling process.

We begin by discussing the role of ethics in the formation of trust. We claimed earlier that trust is based on an assured belief that another person displays integrity, veracity, justice, and other aspects of ethical behavior, and will continue to do so.[43] The dictionary defines ethics as "a particular system of principles and rules concerning duty."[44] When a participant communicates that he has chosen some system of principles and rules, he gives others the opportunity to decide whether or not to trust him. Many professions, including doctors, lawyers and priests, have embraced strong privacy protection in their ethical codes.[45] Other professions with a shorter history of respect for privacy

---

which information is relevant to the case. For a discussion of trust in the context of the clinical medical research, see Francis H. Miller, *Trusting Doctors: Tricky Business When it Comes to Clinical Research*, 81 B.U. L. **REV Y** (2001) (discussing physicians' financial and professional conflicts of interest in clinical trials of new drugs and devices).

[42] A survey done by Princeton Survey Research Associates for the California HealthCare Foundation found that fifteen percent of patients nationally did something "out of the ordinary" to protect their medical privacy, and two percent refused to seek care altogether. *See* Princeton Survey Research Associates, *Confidentiality of Medical Records: National Survey* (1999) (visited February 3, 2001) <http://ehealth.chcf.org/view.cfm?section=Consumer&itemID=1859>. *But see* Nancy J. Moore, *Limits to Attorney-Client Confidentiality: A "Philosophically Informed" and Comparative Approach to Legal and Medical Ethics*, 36 CASE W. RES. L. REV. 177, 188 (1986) (arguing that, even without assurances of privacy (i.e., through physician-patient confidentiality), most patients would sufficiently disclose information to their physicians).

[43] *See* text accompanying note 24.

[44] "Ethics: 1. The discipline dealing with what is good or bad or right and wrong or with moral duty and obligation; 2.a. A group of moral principles or set of values; b. a particular theory or system of moral value; c. the principles of conduct governing an individual or a profession: standards of behavior." MERRIAM-WEBSTER'S 3RD INTERNATIONAL DICTIONARY, *supra* note 7, at 780 (3d ed. 1986).

[45] *See generally* Moore, *supra* note 42 (comparing the ethical requirement of client confidentiality in the legal and medical professions); Seymour Moskowitz & Michael J. DeBoer, *When Silence Resounds: Clergy and the Requirement to Report Elder Abuse and Neglect*, 49 DEPAUL L. REV. 1 (1999) (discussing clergy-parishioner confidentiality). Note however that Moskowitz and DeBoer point out that the clergy does not have a strong

have also incorporated privacy into their codes of professional responsibly. For example, the Association for Computing Machinery ("ACM") code of ethics requires that privacy be considered when designing new systems.[46]

We now move to the role of privacy in trust. We build our own definition of privacy on what we consider the most elegant definition, "informational self-determination," which refers to a person's ability to control the flow of his own personal information.[47] There are two ways in which this self-determination can be achieved: (1) anonymity and (2) fair information practices.

Anonymity protects information by simply not allowing its disclosure, and offers very powerful control over the re-distribution of information. Total anonymity is difficult to achieve, and may not even be desirable in all situations. If information is collected, a variety of "fair information practices" control the information. These practices are sometimes enacted into laws, and the content of what constitutes fair information practices continues to evolve.[48] While these practices differ from instance to instance, there are a number of

privacy protection in their codes and that this privacy protection arises mostly from moral judgment. *See id.* at 5.

[46] One of the ACM's "general moral imperatives" is to "respect the privacy of others." *See ACM Code of Ethics and Professional Conduct Rule 1.7 (1992)* (last modified Jan. 16, 1998) <http://www.acm.org/constitution/code.html>. Many professional association ethics codes include privacy/confidentiality clauses. *See, e.g.*, *Center for Study of Ethics in the Professions*, *Codes of Ethics Online* (visited February 3, 2001) <http://csep.iit.edu/codes/index.html> (displaying the Illinois Institute of Technology's Center for Study of Ethics in the Professions' large, searchable collection of professional codes).

[47] *See* Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1326 (2000), citing Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734 (1987) (discussing the 1983 West German Federal Constitutional Court decision, the National Census Case, which claimed that "unrestricted access to personal data imperils virtually every constitutionally guaranteed right"). Reidenberg points out a slight difference between the German court's concept and the American formulation, which "accord[s] control over the disclosure of personal information." *See* Reidenberg, *supra* note 47, at 1318, citing ALAN F. WESTIN, PRIVACY AND FREEDOM xiii (1967) (discussing Westin's study for the Association of the Bar of the City of New York).

[48] The first Fair Information Practice principles were the Health, Education, and Welfare principles. *See* RECORDS, COMPUTERS AND THE RIGHTS OF CITIZEN, *supra* note 11. These principles motivated the Privacy Act of 1974. *See* The Privacy Act of 1974, 5 U.S.C. § 552 (2000). For more recent principles, see COUNCIL OF THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, (September 23, 1980); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31; Personal Information Protection and Electronic Documents Act, 23 C. Gaz. 1, ch. 5 (2000) (Can.). Each principle was created in part as a response to earlier laws and policy proposals.

criteria that must be satisfied. These criteria are abstracted from sources like the US Privacy Act,[49] or the European Union Data Protection Directive,[50] and include: (1) Notification (the collection of private information may not occur without the knowledge of the information's owner); (2) Choice (the information gatherer must offer the owner of that information an opportunity to refuse to consent)[51]; (3) Minimization (the information gatherer may obtain only as much information as is needed); (4) Use (the information gatherer may only use the information for the express purpose for which he gathered it); and (5) Security (the information gatherer must erect a system to ensure that the other four criteria are not missed due to negligence).[52] Clearly, when these principles are extracted from a relevant law, they may not be arbitrarily violated.

However necessary, policies and agreements are not always sufficient to create a relationship of trust. The systems that surround those policies need to be well designed with privacy in mind.

III. DESIGN IS NOT NEUTRAL

The design, introduction, and adoption of new technologies is a complex and much studied process. The role of privacy in the process, however, has not (as far as we know) been examined quite so thoroughly. Many new systems are apparently designed with little thought to their effect on privacy. Examples considered below include GPS units in rental cars, road toll systems, frequent-buyer cards, and the storage of shipping records. Each of these systems has a substantial and real cost in privacy that was apparently not considered in designing the system. We start with a set of offline scenarios, and then consider an online counterpart.

A. *Toll Roads*

Road toll systems, such as New York's "EZPass," are designed to relieve

---

[49] 5 U.S.C. § 552(a).

[50] *See* Directive 95/46/EC of the European Parliament, *supra* note 48.

[51] Later critiques of the Fair Information Practices pointed out that consent must be meaningful; give us your data or we won't serve you is not meaningful consent. For example, many US health insurers require you to consent to their complete data sharing practices as a condition of receiving care.

[52] *See, e.g.*, U.S. West v. FCC 182 F.3d 1224 (10th Cir. 1999) (holding that asserting a broad interest in privacy is not sufficient to justify a restriction on commercial speech); 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, 1051 (2000) (arguing that contractual privacy protection is constitutionally sound while broader information privacy rules are probably not and that creating free speech exceptions to accommodate such rules could have repercussions); Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1560 (2000) (describing Volokh's article as "masterful").

congestion on major roads while allowing for revenue collection. Although it is the state that collects the highway revenue, EZPass is owned by a private entity. The system has become a locus for subpoenas in divorce proceedings and other civil actions and will likely also become a focus for criminal law enforcement efforts as well. It is unclear whether the State anticipated this initially, although the New York State Police apparently opposed a proposal requiring that such information be subject to subpoenas. Regardless, the system is vulnerable to subpoenas because it has a central database. There is no notification or privacy policy posted on EZPass's homepage.[53] The frequently asked questions section offers no privacy information, and we believe that this makes it impossible to answer adequately any[54] other questions about use or choice. The system is coercive in nature, insofar as toll systems become more efficient and failure to participate in the program results in a substantial cost in time. According to the EZ Pass website, anonymous accounts are not available in most of the jurisdictions which deploy the system.[55]

B. *Frequent-Buyer Cards*

Frequent-buyer cards, like those that supermarkets offer, are often presented to the user as "free," and few people consider the card's impact on consumer privacy. Supermarkets encourage use of the cards by requiring the customer to present their card to benefit from discounts and specials. There is at least one case, however, of "secondary use" of frequent-buyer card information in which the Vons supermarket chain informed a Los Angeles man that Vons intended to use information in their database about his alcohol purchases as part of their defense in a lawsuit.[56] There is no notification of the data storage or potential impact on privacy in many of these frequent-buyer systems and an analysis similar to the EZ Pass system thus applies. We add, however, that unlike the EZ Pass system that from the beginning offered system benefits only to members, the typical supermarket used to offer the same discounts to everyone, not just the cardholders.[57]

All systems impose some requirement for the amount of identification

[53] *See EZPass Homepage*, (visited February 5, 2001) <http://www.e-zpassny.com>.

[54] *See EZPass FAQ Section*, (visited February 5, 2001) <http://www.e-zpassny.com/static/faq/index.html>.

[55] *See EZPass Homepage* (visited February 5, 2001) <http://www.e-zpassny.com>.

[56] *See* Shelby Gelje, *Joining a Buying Club? Your Purchases Might Raise Flags*, SEATTLE TIMES, Sept. 6, 1998 at L5 (describing Robert Ramirez' Rivera's suit against Vons and his claim that Vons representatives threatened to use electronic records of his alcohol purchases against him). Rivera's case was thrown out early in 1999. *See* Stuart Silverstein, *Shopper's Suit Thrown Out*, L.A. TIMES, Feb. 11, 1999, at C2.

[57] Actually, its not clear if EZPass offers a free-rider benefit to those who don't have the system by causing back-ups to be shorter, if the (fewer) non-EZPass lanes end up with more delay, or if the system is neutral for its non-users.

needed, ranging from none to quite a bit. Consider the degree of identification that a system requires as a scale, from complete anonymity to completely verified identity. We assume for now that the latter is possible. Points along this line express the degree of identification a system creates, and we refer to this as their "nymity." For example, cash is untraceable and unlinkable, and often carries with it complete anonymity. If there are video cameras present, then there is less privacy. A phone card is trivially linkable, and with effort, traceable to an individual by calling patterns. Using a credit card to pay for calls is more easily traceable, as the card has a name affiliated with it. In creating a system, it is easy to move it towards verified identity, and hard to move away from it. Once the system relies on having identity verification, it is difficult to recreate the same system without that component of identity verification. Thus, the nymity graph, when applied to real systems, is a *slider* during the design phase. The implementation, however, transforms it into a nymity *ratchet*. Good system design should thus aim towards the anonymous end of the slider to preserve flexibility with respect to new system requirements.[58]

C. *Amazon.com*

Amazon.com was one of the first e-tailers to consider issues of privacy in a prominent way.[59] They issued a privacy policy with quite a few promises in it.[60] It is unclear whether this elaborate privacy policy helped their phenomenal rise. More recently, Amazon.com issued a new privacy policy that removed some of those protections.[61] This will have a substantial impact on the ability of companies to make believable promises—this is akin to a

---

[58] *See* Ian Avrum Goldberg, A Pseudonymous Communications Infrastructure for the Internet (2000) (unpublished Ph.D. dissertation, University of California (Berkeley)) (on file with author).

[59] *See* Valerie Lawton, *Net Firms Must Assure Privacy*, TORONTO STAR, April 3, 1998 at E2 ("[Ontario privacy commissioner Ann] Cavoukian notes one of the most successful Internet merchants—bookseller Amazon.com—has strong privacy policies, including a promise not to sell lists of what people are buying."); Ellen Messmer, *New Wave of 'Net Marketing' Invades Consumer Privacy*, NETWORK WORLD, Oct. 21, 1996 at 42 (noting, in 1996, that "some Websites, such as 'Net bookseller Amazon.com Books, do post privacy policies and provide a way to opt-out, but most still do not").

[60] "Amazon does not sell, trade, or rent your personal information to others." *See Electronic Privacy Information Center*, *Old Amazon.com Privacy Notice (prior to September 2000)* (visited February 1, 2001) <http://www.epic.org/privacy/internet/amazon/old_policy_0900.html>.

[61] "In the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets." *Amazon.com Privacy Notice*, *supra* note 5; *see also* Tamara Loomis, *Amazon Revamps Its Policy on Sharing Data*, N.Y.L.J. Sep. 21, 2000, at 5 (noting a change in the privacy policy from assurances of nondisclosure of customer data to a warning that data may be sold as an asset of company).

defection, and destructive of trust. As of this writing, it is unclear if the Federal Trade Commission will initiate action to force compliance with the old policies. Such action could offer a degree of reliance.

CONCLUSION

Trust can appear in a situation where mutually suspicious players have no recourse to authorities. This situation is analogous to the situation that exists on the Internet. Demonstrated ethical behavior on the part of various players can help to overcome the mistrust, and ensure that players choose to interact with each other. Investment in privacy is one such demonstration of ethical intent. Companies who wish to avoid the alternatives have begun to address the need for ethics in design and implementation. Merely asserting trustworthiness, however, is not likely to convince today's cynical consumers. Companies will need to start building systems that show their interest in behaving ethically because only then will they be trusted.