Helen Nissenbaum

Can Trust be Secured Online? A theoretical perspective

Introduction

Two concerns animate much recent literature on the subject of trust online -- in research journals, trade magazines, news and government reports. One is a concern over building adequate security systems, the other, is a concern over e-commerce. Technical experts in security warn that the vast networked information system (the network of networks that includes local private systems in addition to public systems like the Internet, the Web, Cyberspace) is vulnerable to technical failure as well as malicious attack. To induce users to trust the system we must build strong mechanisms of security to create «trusted», or rather, trustworthy systems that overcome both types of vulnerabilities. Proponents of e-commerce, spurred by an interest in sustaining active commerce online, advocate in favor of technology and practices that would induce consumers to trust providers of goods and services, would induce providers to trust consumers, and in general, would create a general climate of trust online. Consumers must not be fearful that they will be cheated, defrauded, have their credit card numbers stolen, or receive poor quality goods; providers must not be fearful that people will fail to pay, or repudiate their commitments. Each must not fear that those with whom they transact will, somehow, reach out and harm them or their property.

Although the two concerns differ in that one is primarily focussed on the technology and the other, primarily motivated by a particular use, they have in common a vision of the likely shape of the solution; namely, a suite of tight technical security mechanisms. So conspicuous has been the vision of trust through security portrayed by these two groups that it now occupies the mainstream – in part because there are no equally persistent, competing interpretations and in part, because talk of trust online is relatively new and the mainstream view relatively uncontested. This essay is an evaluation of the vision of trust through security. Drawing on important insights on

trust in general of philosophers, social scientists and social theorists, I argue that the online landscape this vision would produce would not be conducive to trustworthiness or trust. It fails because it is founded upon on a conceptual misconstrual of trust. Although this critical evaluation is not followed by a full-blown alternative, it demonstrates how theoretical insights can, and should, inform practical efforts to induce, promote and nurture trust online.

When speaking about trust in the online world, we could be referring, in the broadest sense, to a technological system so vast and powerful that it sits now at the hub of almost all other parts of the critical infrastructures mediating significant aspects of social, community, cultural and political life and controlling and in some cases conjoining fundamental infrastructures, including energy, commerce, finance, transportation, education, and communication. Here, I focus attention on the conditions of trust not in the context of the system as a whole and in the vast and powerful grid that connects and controls satellites, nuclear devices, energy, the stock exchange, and so forth. I am concerned with trust in context of those parts of the system that are directly experienced by the ordinary people, who in increasing numbers, use it to talk, conduct business transactions, work, seek information, play games, and transact with public and private institutions. Presently this means the World Wide Web (the Web) and the various servers (computers), conjoined networks, people, and institutions that comprise it.

Neither does this essay cover everything that *trust* online could mean. Trust is an extraordinarily rich concept covering a variety of relationships, conjoining a variety of objects. One can trust (or distrust) persons, institutions, governments, information, testimony, deities, physical things, systems, and more. Here, I will be concerned with trust as a relationship between one person (a trustor) and another (the trustee). Although, in practice, the trustee position could be filled by almost anything, here I limit consideration to cases where the trustee is a being to which we are willing to ascribe intentions, motivations, interests, or reasons, and might also refer to as «agents». Central to this category, I would place people – individually and in groups. But I would also be willing to include organizations, communities, and institutions. Excluded from my discussion, therefore, will be at least

one quite common reference to trust in the online context, namely, trust in the networked, digital information systems themselves, in the layered hardware and software that comprise the micro-systems individually and the macro-system that is formed by these. My reasons are pragmatic. These cases are sufficiently different from on another that they deserve separate (but equal) treatment.

The Function of Trust

It is not unfair to question why we care about trust online. Such a question provokes two lines of response. One is to elaborate on the function and value of trust, generally. We care about trust online because trust brings about valued ends, generally, and consequently is good for the online world as well. This section addresses the function and value of trust. The second reason for caring about trust online – the subject of the next section – is that the online context deserves special attention. Because the world online is distinctive in ways that are relevant to trust, we should examine these differences and their implications for trust.

There is an unexamined sense that trust is a good. Meaningful relationships rest on trust; families, communities, societies, and political institutions work better in a climate of trust. Scholarship endorses this sense of trust's function and importance. It reveals the benefits of trust not only for individuals – those who trust as well as those who are trusted, but also for relationships between and among people, and for groups structured as institutions, communities, societies, and so on. I draw on a few brief samples from the extensive literature on trust to illustrate the various functions trust is ascribed.

Niklas Luhman, a social theorist whose profound work on trust has been widely influential, characterizes trust as a mechanism that reduces complexity and enables people to cope with the high levels of uncertainty and complexity of contemporary life. Trust makes the uncertainly and complexity tolerable because it enables us to focus on a few possible alternatives. Humans, if faced with a full range of alternatives, if forced to acknowledge and calculate all possible outcomes of all possible decision nodes, would freeze in uncertainty and indecision. In this state, we might never be able to act in situations that call for action and decisiveness. In trusting, Luhmann

says, «one engages in an action as though there were only certain possibilities in the future.» (20) Trust, further, enables, «...co-operative action and individual but coordinated action: trust, by the reduction of complexity, discloses possibilities for action which would have remained improbable and unattractive without trust-- which would not, in other words, have been pursued.» (25) According to this account, trust expands people's capacity to successfully relate to a world whose complexity, in reality, is far greater than anything we are capable of taking in.

Trust's rewards extend beyond the individual. Enhancing relationships, trust also facilitates opportunities for discovery and creativity.

The possibilities for action increase proportionately to the increase in trust --trust in one's own self-presentation and in other people's interpretation of it. When such trust has been established, new ways of behaving become possible; jokes, unconventional initiatives, bluntness, verbal short cuts, well-timed silences, the choice of delicate subjects etc. When trust is tested and proven in this way, it can be accumulated by way of capital. (40)

This idea of trust as capital -- social capital, has been echoed, developed, and popularized by Robert Putnam in his study now classic study of Italian civic society. (Putnam, 169-170) With each trust affirming action, trust accrues within communities as capital, there to tap in troubled times. Other political philosophers have explored ways in which trust benefits societies and the associations within them. Philip Pettit, for example, stresses the strength and solidarity that trust can engender: «…it is now common wisdom that trust is a precious if fragile commodity in social and political life.» (225); it is characteristic of flourishing civil societies (Pettit, Putnam). Trust among citizens may be the magic ingredient that helps undergird political and civil stability in multicultural societies (Weinstock); trust is an "important lubricant of the social system» (Arrow quoted in Seligman, 75); it is the basis for modern solidarity (Seligman). Trust by individuals of institutionalized authority, such as government, may prevent a citizenry's disengagement from the system, and may even prevent highly volatile and disruptive reaction to harms perceived to come from these authorities (Becker).

Emerging from these and other works is the idea that trust is especially needed in complex, varied, and somewhat unpredictable, personal, social and political contexts. Trust facilitates cooperation and success within civil and political society; it enriches people's lives by encouraging activity, boldness, and adventure and by enriching the scope of individuals' relationships with others. It is not surprising, therefore, that an interest in trust should grow just as the realm we known as Cyberspace, the Internet, the Web, the Global Information Infrastructure, burgeons, just as it crosses a threshold of complexity where individual participants are faced with a multiplicity of possible interactions, relationships, community, offerings and experiences; just as it is beset by deep and difficult questions about authority and governance.

Trust promises the same benefits online as off: namely trust improving people's experiences and relationship, improving communal and civic life, and stabilizing governance. We can expect that more people and institutions will «buy in» to the online world, will engage with others online, if there is sufficient trust. If a climate of trust can be established on the Net, and attitudes of trust toward partners in electronically mediated transactions, then the online world will thrive, it will attract information, it will be lively with interaction, transaction and association. This thriving will attract further investment of all kinds, which in turn will fuel participation, and so on. Conversely, if people do not trust interactions mediated electronically, they will minimize them; they will be cautious and suspicious in their dealings, they will not place information and creative works on the web, they will not engage in E-commerce, they will not indulge in MUDS, MOOS, E-lists, B-boards, Listservs, chatrooms, buddy lists, electronic banking, and more. A great resource will be wasted.

The Conditions of Trust Online and Off

Given all that seems to be at stake in promoting trust and trustworthiness online, what, if anything, stands in the way of simply extending the conceptual insights and practical wisdom of research and scholarship into the online arena? Although, ultimately, this is a promising strategy, there is considerable ground to clear. Concern over trust online is prompted not only by an appreciation of the value and function of trust, in general, but by the impression that the online

landscape poses particular challenges to forming and sustaining trust. The online world is a new phenomenon and novelty, or unfamiliarity, in itself can stall the formation of trust. Beyond sheer novelty, however, there are more intractable differences between online and offline contexts that are particularly relevant to the formation of trust. Before identifying the obstacles in the way of trust online, let us review common wisdom and scholarship on the subject of the formation of trust in general.

Questions may prompt our inquiry: What mechanisms govern trust? To what factors are people's tendencies to trust systematically responsive? What influences people's judgments that other people, groups, and institutions are worthy of trust?. A common set, which we may think of as cues, clues, or evidence of trustworthiness, seem crucial to whether people decide to trust, or form trusting attitudes. Inducing, or eliciting trust, these cues may also nurture or sustain it. These clues may induce or elicit trust as well as nurture and sustain it. The ones I have chosen to discuss below reflect my specific concern with trust in the online world.

History and Reputation

One of the most convincing forms of evidence that others merit trust is their past behavior. If they behaved well in the past, protected our interests, did not cheat or betray us and, in general, acted in a trustworthy manner, they are likely to elicit trust in the future. If they have not fulfilled past hopes, then we will tend not to trust them. Where we have not built a history of direct interaction with others, we may learn indirectly about their trustworthiness from the experiences of others, or be influenced in our judgments even more remotely through their reputations.

Inferences Based on Personal Characteristics

A trusting attitude may be based on the presence of perceived qualities of the other. Philip Pettit identifies four: virtue, loyalty, prudence and a desire for the good opinion of others. That is to say, these qualities influence whether a person will trust their subjects. Pettit writes,

To be loyal or virtuous or even prudent is, in an obvious sense of the term, is to be trustworthy. It is to be reliable under trust and to be reliable, in particular, because of possessing a desirable trait. (211)

The fourth quality, namely, a desire for the good opinion of others, though less deserving of our admiration, is nevertheless a powerful mechanism for preventing betrayals of trust (203). Accordingly, Pettit recommends against calling the person who chases good reputation trust*worthy*, preferring a more modest commendation of trust-*responsiveness*, or trust-*reliance*. Though not in direct disagreement with Pettit, Adam Seligman offers a different perspective, drawing attention to the importance of familiarity, similarity and shared values as triggers of trust. What we know about someone, what we may infer on the basis of «their clothing, behavior, general demeanor,» (69) may lead us to judgments about their values and moral commitments, especially telling if we judge them to be similar to ours. A common religious background, a high school, a neighborhood, a traumatic experience (e.g. fought in a war), affects how confident we are in predicting what others will do, how comfortable we are to rely on them.

Relationships: Mutuality and Reciprocity

Aside from personal qualities, the relationship in which one stands to another might bear on the formation of trust. The presence of common ends can stimulate trust. Such cases of mutual ends occur when a person is «in the same boat» with another. When I fly in an airplane, for example, I place trust in the pilot partly because he is in the plane with me. I presume that we have common, or confluent ends; our fates are entwined for these few hours in which we fly together.

Reciprocity is slightly different but it, too, can be grounds for trust. In a reciprocal relationship, we trust others not because we have common ends but because each of us holds the fate of others in our hands in a manner of tit-for-tat. This may occur, for example, when people are taking turns. The agents whose turn is first, deals fairly, or reliably, or responsibly with the other because soon the tables will be turned. The relationship of reciprocity admits of great variability. In some cases, there is clear and imminent reversal of roles (today I drive your kids, tomorrow, you drive mine), in others it is more generalized. Thus, I might donate money to the Cancer Foundation hoping that when I am

ill, these funds will somehow help me. Robert Putnam highlights the role of reciprocity in communities which are blessed with a climate of trust. Citizens help those in need with the expectation that when they are need, others will help them. (Putnam, 171-176)

Role Fulfillment

There is another, perhaps more compelling reason for trusting the pilot of my airplane. After all, the pilot would not trust me despite our common interest in of staying alive. Crucial to my trusting the pilot is that he is a pilot and all that being a pilot within the framework of a familiar system means. I know what pilots are supposed to do. I am aware of the rigorous training they undergo, the stringent requirements for accreditation and the status of airlines within a larger social, political and legal system. Several of the authors already mentioned have discussed the importance of roles to the formation of trust. (See Baier, Pettit and Seligman)

Contextual Factors

Beyond what we know about the other, which may or may not be decisive in eliciting trust, features of the context in which we operate can affect our readiness to trust. A setting in which betrayal and fidelity are routinely publicized, for example, would be more conducive to trust-reliance, and consequently trust, than a setting in which people can effectively hide their deeds – especially misdeeds. A setting in which rewards and sanctions follow trustworthiness and betrayals respectively will induce trustworthiness and trust. Where sanctions and rewards are not possible, a community can provide other modes of approbation and disapprobation for trustworthy and untrustworthy behavior respectively through such means as publicly articulated norms, character education, parables, and so on. (Luhman, 84) And if all else fails, a society might set in place forms of «trust insurance» to act as a safety net for those whose trust is betrayed.

Obstacles to Trust Online

The online world differs from the offline world in ways that are relevant to trust. In particular, it obscures or lacks entirely the dimensions of character and personality, nature of relationship, and institutional

character on which we normally rely to form attitudes or base decisions about trust. Consider three prominent cases: 1) identity; 2) personal features; 3) role definition.

1) Missing Identity

In its current design, the medium offers individuals numerous ways to cloak, or obscure identity. Agents are not compelled to relinquish the identities of their off-line selves in many of their online transactions. Although anonymity offers enormous benefits, it reduces the range of cues upon which people base judgments of trust. Referring to the principles mentioned above, we can see why identity is important to trust: identity is the string upon which we thread the history of interactions with another. Without this thread we lack the traditional means of referring to past experiences either of vindicated trust or of betrayal. Lacking information about a sustained identity means we are also deprived the means of learning from the experiences of others whether an agent is trust reliant. Lacking knowledge of an agent's sustained identity means, also, that the usual means of reasoning based on a reciprocal arrangement cannot be developed. Finally, because identity is also bound up with accountability, people might presume that anonymous agents are less likely to act responsibly. As a result they would be less inclined to trust. And where identity is lacking, our usual means of enforcing accountability cannot be expected to work.

2) Missing Personal Characteristics.

There is an opacity not only with respect to others' identities, but with respect to many of their personal characteristics which affect (heighten or diminish) attitudes of trust. We are separated from others in time and space; we lack cues that may give evidence of similarity, familiarity, or shared value systems. We may not know the other's gender (male, female, or «other»), age, race, socioeconomic status, occupation, mode of dress, geographic origins, nor some of the bodily signals that serve as cues in interactions where others are physically proximate. Are we communicating with a 14 year-old girl or a 57 year-old man posing as a 14 year-old girl? Are we selling a priceless painting to an adolescent boy or to a reputable art dealer? Are we sharing a virtual room with an intriguing avatar or a virtual

rapist? (Dibbell) We must transact and depend on others who are separated not only by distance but also by time, who are disembodied in many of the ways that typically contribute to our sense of their trustworthiness.

3) Missing Role Definition.

The online world is novel not only for the individuals who must place their trust in it and the interactions mediated by it, but for the individuals, groups, and institutions who must prove themselves worthy of, or meriting trust. The novelty and difference is not something simply to be overcome, to be gotten over, for it is these differences and this novelty that is touted as the boon of the online world. Enthusiasts invite you to participate in it *because* it is new, different, better, seamless, immediate, unstuffy, truly democratic, and so forth. To the extent that the online world is sui generis in these ways, however, it undermines the powerful mechanism of traditional role definition. We do not yet have in its place the mutually understood systems that define and support roles. While some of the traditional roles appear to have shifted online (e.g. the shopkeeper) these, nevertheless are different in ways that may be unsettling. We are not certain whether our expectations of them are supported in precisely the same way as they are offline. Besides those that appear similar, there many new functions and new roles: online casinos, online communities, «sysops», avatars, bulletin board moderators, and so on, whose natures are not yet formulated and almost certainly not commonly recognized among all citizens of the online world.

Securing Trust through Safety

Under conditions where many of the usual cues of trust and trustworthiness are missing or obscured, how do we sustain trust online? The answer to this question that many people support promotes security and safety as the panacea. Supported by security experts, security-minded systems managers, government oversight bodies and espousers of e-commerce, this answer holds as its objective a perfected toolkit of security mechanisms as the key to ensuring safety for sanctioned participants of the online world. The toolkit would protect these participants against harm to them, their computers, and their information.

Concern over computer security is almost as old as computing itself. For decades pursuit of security technology has grown side by side the growth of computing and has expanded and changed shape in response to numerous changes in computing as well as its application. Conceiving of trust as one of the guiding principles of security technology, however, is a recent phenomenon. Considers some of the ways that security mechanisms function to remedy the loss of cues and clues that appears to be an inevitable condition of the online context: 1) Access Control; 2) Transparency of Identity; and 3) Surveillance.

1. Access Control (Insiders versus Outsiders)

One of the earliest worries that security experts had to face even when computers served as stand-alone calculators and repositories of information was guarding access to and the integrity of systems and information. This meant keeping unauthorized agents out, while allowing authorized agents in. This need has persisted even as the technology has developed, especially in the wake of networking and greatly increased potential for interactivity among online agents. Interactivity means greater capacity of unsanctioned access and damage: viruses carried via emails, evil Websites, applets that cause harm; and information damaged or stolen while in transit. Security experts offer a suite of mechanisms to protect against unwanted access including passwords; «firewalls» (barriers around systems intended to make them impermeable to all but sanctioned access); and various applications of cryptography to protect the integrity and privacy of information held in computers and in transit across networks.

2. Transparency of Identity

Another means of securing systems and networks is through greater transparency of identity. To begin with, identification is a necessary complement to access control because controlling access because controlling access hardly ever means preventing anyone from using a system or information but involves, rather finding a way to distinguish, reliably and accurately, between authorized and unauthorized agents. Identification serves also to distinguish between those who are deserving of or have rights to certain online goods and services. It

increases the possibility of holding agents accountable, and for identifying perpetrators when harm is discovered. For these reasons, and others, transparency of identity is important.

Proposed methods of attaining transparency of identity are numerous and vary according to needs. For the cases where a strong link is needed between a virtual agent and a physical person, security experts have, for example, pursued strategies for biometric identification (e.g. through fingerprints, DNA profiles, retinal images.) For purposes of authenticating persons, computers, or institutions as sources of action or information, cryptographic techniques offer an array of possibilities such as digital signatures and digital certificates. A further application of these mechanisms ensures non-repudiation by agents of commitments or promises they may have made.

3. Surveillance

Overlaid upon the security offered through access control and transparency of identity, there is a third layer, namely security through surveillance. Whether by actively watching or tracking actions and transactions, or by passively recording (reifying) digital trails, mechanisms of surveillance offer the prospect of preventing harms as well as apprehending perpetrators after harm has been done. Technically, surveillance may take the form of «intrusion detection» where a real-time monitoring system can issue an alarm in response to suspicious activity. It can also take the form of logging and auditing which creates records of activity that can be sifted through and studied at a later time. Logging and auditing helped authorities identify the alleged creator of the Melissa virus.

Evaluating the Idea of Trust Through Security

The claim on behalf of the science and engineering of security is that the closer we can get to perfecting a suite of mechanisms for controlling access to systems and information, for acquiring reliable markers of identity, and for maintaining a watchful eye, the closer we will get to a world worthy of trust. We will attain trust through security. This claim has prima facie plausibility because many of the mechanisms function precisely to restore many of the clues and cues lost to appraisal in the online world. This is most easily seen in the

mechanisms of identification provides information about the agents with whom people interact and thereby restores some of the cues and clues, including in some cases information about the past record of an agent. These mechanisms also allow for the creation of reliable online reputations. Assuring non-repudiation restores accountability, as does surveillance.

Despite the promise, and despite the clear benefits security promises, I will argue as a means of engendering trust, security cannot provide the complete answer. The prevailing rhetoric that places full confidence in the attainment of trust through security is misguided not because security, appropriately used, is a misguided effort but because when the proponents of security and e-commerce would bind trust too closely to security they threaten to usurp a concept as rich and complex, as intensely social, cultural and moral, as trust, for merely one slim part of it. The mistake is not merely semantic; it has weighty practical consequences. Pursuing trust online by pursuing the complete fulfillment of the three goals of security would no more achieve trust and trustworthiness, online -- in their full blown senses -- than prison bars, surveillance cameras, airport X-ray conveyers, body frisks, and padlocks, could achieve offline. For the ends envisioned by the proponents of security and e-commerce are contrary to core meanings and mechanisms of trust.

Interpreting trust as security is inadequate in at least two ways: one is that it could lead to a climate that is hostile, not friendly to trust. Interpreting trust as security will diminishes the «quality of life» in the online world by diminishing critical opportunities for forming and nourishing trust. The second problem with this interpretation is that, as currently conceived, pursuing trust through security contributes toward a status quo that misses some important requirements of trust online because it still leaves the door open to a broad range of trust-undermining actions. In order to develop these ideas, we need to refer, once again, to theoretical insights.

The Nature of Trust

Trust is an attitude. It is almost always a relational attitude involving at least a trustor and a trustee. In the relation of trust, those who trust accept their vulnerability to those in whom they place trust. The realize

that those they trust may exercise their power to harm, disappoint, or betray; yet at the same time they regard those others «as if» they means well, or, at least, mean no harm. Trust, then, is a form of confidence in another, confidence that the other, despite a capacity to do harm, will do the right thing in relation to the trustor. The philosopher, Annette Baier characterizes trust as «accepted vulnerability to another's possible but not expected ill will (or lack of good will) toward one» (235); trust is the «reliance on others' competence and willingness to look after, rather than harm, things one cares about which are entrusted to their care.» (259) For Russell Hardin, it is quite simple, «…virtually all writers on trust agree, trust involves giving discretion to another to affect one's interests.» (507) In a similar vein, Adam Seligman holds trust to be «some sort of belief in the goodwill of the other, given the opaqueness of other's intentions and calculations.» (43)

Whether trust is a species of belief (or expectation) or a non-cognitive attitude is a matter of some disagreement. Those who hold it to be a species of belief are more likely to subject it to judgments of rationality or irrationality. But, like Becker, even those theorists who hold it to be a non-cognitive attitude agree that it is systematically responsive to evidence as well as the variety of cues and clues discussed earlier. Although for purposes of this essay, we do not need to take a stand on the question of belief versus non-cognitive attitude, we draw (have drawn already) on both empirical and analytic work linking trust systematically with the presence or absence of various cues.

Securing Trust versus Nourishing Trust

Let us now turn to the first critique, namely, that that pursuit of trust through security may actually quash trust. How so? Common to all the works on trust that I studied was a recognition that trusting involves vulnerability. When people trust, they expose themselves risk. Although trust is not usually groundless, it involves no guarantees. The cues, clues, and triggers may give evidence of the reasonableness of trust but they do not, cannot, amount to certainty. (Pettit, Luhmann, Weinstock.) As Hardin writes, trust is «inherently subject to the risk that the other will abuse the power of discretion.» (507) Where people are guaranteed safety, where they are protected from harm via assurances, as when the other acted under coercion, for example,

trust is redundant, trust is not needed. What we have is certainty, security, safety – not trust. The evidence, the signs, the cues and clues that ground the formation of trust must always fall short of certainty; trust is an attitude without guarantees, without a complete warrant. When we constrain variables in ways that make things certain – safe -- we are usurping trust's function. Trust is squeezed out of the picture.

No loss, some, like Richard Posner, would say: «But trust, rather than being something valued for itself and therefore missed where full information makes it unnecessary, is, I should think, merely an imperfect substitute for information.» (Posner, 408) According to this position, if we must choose between trust (and vulnerability) on the one hand, and certainty, on the other, then surely certainty wins. In the online world, however, the costs of certainty are considerable.

In an environment as extensive, rich and complex as the online world, aiming for safety and certainty above all has a price – namely, limitation. We do not have the means at our disposal of assuring safety at the same time that we are able to benefit from the full richness, opportunity and complexity. The former would require simplification and constraint. It would mean curtailing the scope and nature of interaction; would a priori judgments about whom we will interact with and whom not. It would involve opening ourselves up to greater transparency and surveillance. The choice is not, at least yet, between a secure Cyberspace and an insecure, unsafe one. The cost of a perfectly secure Cyberspace is a limiting and constraining of what people can do online, the range and nature of activities allowed to them, the freedoms they can experience, and the complexity of relationships and community they can build.

When scholars of trust say that trust involves vulnerability or risk, they can be understood as making more than conceptual claims about trust. They may, of course, be interested in saying something about the sense contained in the notion of trust, that whatever attitude a person has it cannot be trust if it involves no vulnerability, but they may also be offering conjectures on the empirical nature of trust, its conditions, its causes, and its effects. In this second mode, several scholars have suggested that in a context of complete certainty, the conditions needed to induce and nourish trust are absent. Trust will not flourish in a perfectly secure environment for reasons that are very

different from those that explain why trust will not flourish in a hostile, threatening environment. For trust to develop between an individual and either another individual or an organization, the individual must somehow have had the opportunity to test the other agent and have them pass the test. Luhmann, below, explains the crucial role of uncertainty in the process of building trust,

First of all there has to be some cause for displaying trust. There has to be defined some situation in which the person trusting is dependent on his partner; otherwise the problem does not arise. His behaviour must then commit him to this situation and make him run the risk of his trust being betrayed. In other words he must invest in what we called earlier a «risky investment». (42)

When we are placed in a context where we depend on others for our well-being and are assured or guaranteed that these others will not harm us, then the context is a safe and secure one, but not one that nourishes trust. No test has been given; none has been passed. The variables that theorists and empirical scientists have identified as trust-inducing, may signal the reasonableness of trust in a particular setting, but when grounds are transformed into guarantees of good behavior trust disappears replaced not by distrust but, perhaps, by certainty. In the presence of a violent psychopath whose limbs are shackled, one feels not trust, but – at best -- safety.

There is yet another reason to question the efficacy of security in delivering trust. Boxing people in is a notoriously bad strategy for inducing trustworthiness or even trust-reliance. Constraining freedom directly, or indirectly through, say, surveillance may backfire and have the opposite effect. Roderick Kramer notes in his review of empirical work in the social sciences on the effects of close supervision or surveillance in the workplace on trust,

Ironically, there is increasing evidence to suggest that such systems can actually undermine trust and may even elicit the very behaviors they are intended to suppress or eliminate. In a recent discussion of this evidence, Cialdini (1996) identified several reasons why monitoring and surveillance can diminish trust within an organization. First, there is evidence that when people think their behavior is under the control of extrinsic motivators, intrinsic motivation may be reduced

(Enzle & Anderson 1993). Thus, surveillance may undermine individuals' motivation to engage in the very behaviors such monitoring is intended to induce or ensure. (16 of 19)

Pettit reinforces this observation,

…certain intrusive forms of regulation can be counter-productive and can reduce the level of performance in the very area they are supposed to affect. … If heavy regulation is capable of eradicating overtures of trust, and of driving out opportunities for trusting relationships, then it is capable of doing great harm. (225)

The many inducements at the disposal of individuals and institutions to encourage trustworthiness are most effective when they operate indirectly. Above all people need to perceive a choice. By means of these inducements, including sanctions and rewards, clearly articulated norms, education, and character development, etc. we may increase the incidence of trust as well as trust-reliance, but if we go too far, and deny the possibility of choice, we deny what is fundamental to trusting relationships and climates of trust.

Applying these observations to the online context, we would conclude that acceding to surveillance, strong identification, restriction on the range and variety of interaction to ones known to be «safe» and to emanate from reputable people and organizations, and so forth, may yield sufficient assurance and safety to please security conscious individuals. It would probably encourage greater participation in E-commerce. At the same time it would limit the spectrum of possible experiences online. The tradeoff is clear: a more freewheeling, open, permissive online world is likely to be the less safe. Proponents of security would limit the range of interactivity, increase surveillance and transparency – all in the name of trust. I have tried to contrast the safety, assurance, and warranties that is security's goal with the experimentation and risk that are the test-beds for trust. Through security we may create a safer world, inhospitable to trust not because there is distrust, but because trust cannot be nourished in environments where risk and vulnerability are, for practical purposes, eradicated. By trying, as it were, to enforce trust, we make its emergence impossible.

Security is no Panacea

We turn now to the second critique of trust through security. It is this. Even if we were somehow to get past the misgivings discussed above, there remains a considerable question about the promise of security technology, as currently pursued, as the decisive remedy for the precariousness of trust. If the earlier criticism was that security overshoots the mark and creates an environment that does not allow trust to take root and flourish, then this criticism is that security may not go far enough. Even though security mechanisms promises to reduce our vulnerability in some ways, it leaves us vulnerable in other ways that are relevant to the prospects of trust online. This loophole is all the more worrisome because having achieved some modes of safety through security we might fail to notice its significance until considerable damage is done.

To elaborate on this claim, let me set in place a simplification which we can discard in a little while. For purposes of many discussions of security, it is useful to frame what is at stake terms of «insiders» and «outsiders.» Experts in computer security respond to the worry that malicious (avaricious, incompetent) outsiders may break into our online space, compromise or steal information, and destroy or compromise our systems. They develop security mechanisms to keep the outsiders where they belong – outside, and to help spot, or identify outsiders as such, and in order to take appropriate action – preventative or punitive.

Thus far, security mechanisms have not systematically recognized the threats of insiders, those agents (people, organizations, entities) who have traditionally been allowed, by degrees, legitimate access to our spaces. These agents, who count among the respectable, socially sanctioned, reputable members of online society, engage in actions that many citizens of the online world dislike, resent, consider harmful. They track our Web activities, they collect and use personal information without our permission, they plant «cookies» on our hard drives, they fill our mailboxes with spam, and they engage in relentless commercialism. Some of these insiders – perhaps not the «respectable» ones – afflict us with hateful emails («flame»), send us threatening chain mail, and even attack our virtual selves. (See Dibell's «A Rape in Cyberspace.») In other words, even if the walls of

security keep outsiders outside, they do not curtail the harmful intrusions that, behind the veil of respectability and legal sanction, make online citizens skittish, cautious and resentful, intrusions that are fully capable of engendering a climate of suspicion and distrust online even if we are successful in our projects to secure the online world.

A wall of defense against malicious outsiders does not defend against the threats posed by legitimate insiders. Respectable members of the online world who energetically defend their «right» to exercise online freedoms (by means of cookies, misleading registration, matching, mining, and so on) are, I argue, chipping away at trust just as surely as the allegedly amoral hackers. The former, as much as the latter, are capable of causing a dangerous ebb in the abundant social capital we currently enjoy in life online. The results of these small transgressions may not be immediately evident because it is in the nature of trust to be conservative – both to build and to ebb. (Slovic, Becker)

That the transgressions I speak of are capable of undermining trust is implied by several of the works that have shaped this essay. Quite specifically, a long-term study of e-commerce strongly indicates that trust is related to consumers' sense that information about them would be held in confidence by those with whom they transact. (Hoffman, Novak and Peralta). That is, suspicion is directed not only to foreign third-parties but even to familiar parties who deal in ways thought to be inappropriate with personal information. Other works on trust point to variables capable of undermining trust which would appear invulnerable to the familiar suite of security mechanisms. I note, in particular, work that highlights the way intentions and motivations of an agent may affect whether others perceive them to be trustworthy or trust-reliant. Although trust is related to the pattern of relevant past experiences in an obvious way -- positive experiences generally breeding trust, betrayals breeding distrust -- the intentions and motivations of the other party can affect the way these experiences are interpreted. Lawrence Becker convincingly discusses this point. Becker argues that intention, or will, matters even more in the formation of trust than outcome; it is in the goodwill of the other that we trust (or fail to trust). As long as we believe that others are well-intentioned towards us, our trusting attitude towards them will survive a

great deal of bad news: «incompetence, mendacity, greed and so forth.» (51) Even in relation to government, Becker suggests that only when citizens begin to attribute the poor performance of governments to deviant motivations (e.g. corruption or inappropriate power seeking) will they «respond in ways that are … volatile and disruptive». Citizens' trust, it seems, is able to survive incompetence, at least for a while. In a similar vein, Paul Slovic, an expert on risk assessment, reports that the extent to which citizens are willing to accept societal risk due to technological innovation is related to their degree of confidence in the motives of those in charge.

Gaining knowledge of the motives and intentions of others often requires subtle detection and artfulness. Where direct information is not available – as usually is the case -- we infer them from a myriad of indirect sources. Among these indirect sources, the others' interests feature significantly. When, for example, a politician seeking office expresses concern for a particular situation, voters may attribute the expression not to genuine feeling but to an interest in being elected. The public lives of all people are filled with the need to interact, even cooperate, with others whose interests are not consistent with their own and may even conflict. In such cases, we transact cautiously, ever on the lookout for betrayal, or as a collective, we seek protection from betrayals and exploitation. Learning progressively that individuals and corporations wishing to increase their potency benefit from information gathering and numbing commercialism, people will realize that such interests are not consistent with their own. If we choose not to pursue policies for the online world that contain the pursuit of avaricious interests that are contrary to those of the citizens of the Net, we are, I fear, planting the seeds of general distrust. People may continue to participate in this arena, but will do so with caution and a sense of wariness, wisely so, in interactions with those whose interests run contrary to our own and whose actions may be annoying, bothersome, intrusive, or even threatening. Guardedness will be the norm.

Those who would pursue security in the name of trust do us this disservice. They focus on the outsider, the aberrant individual (or organization), the trickster, the evil hacker, the scam artist. These are the villains from which security would protect us. But these techniques

do nothing against the agent, acting behind the veil of respectability, who invades our privacy and offends us by turning Cyberspace to its own interests and not ours. For the lives of the vast majority of Net users, the second and not the first, is the significant danger; the second at least as much as the first, that affects our attitudes of trust online.

References

Abdul-Rahman, Alfarez, and Stephen Hailes. "A Distributed Trust Model." NSPW 1997. Proceedings of the Workshop on New Security Paradigms. 48-60.

Becker, Lawrence C. "Trust in Noncognitive Security about Motives." Ethics 107 (Oct. 1996): 43-61.

Baier, Annette. "Trust and Antitrust." Ethics 96 (Jan. 1986): 231-260.

Backhouse, James P. "Security: The Achilles Heel of Electronic Commerce." Society 35 (May 15, 1998): 28.

United States. Department of Defense. Department of Defense Trusted Computer System Evaluation Criteria. Washington: Department of Defense Standard, 1983. http://www.all.net/books/orange/title.html. Accessed July 1,1999.

Dibbell, Julian. "A Rape in Cyberspace." Flame Wars. Ed. Mark Dery. Durham: Duke University Publishers, 1994. 237-261.

Hardin, Russell, "Trustworthiness." Ethics 107 (October 1996): 26-42

Hoffman, Donna L.; Thomas P. Novak, and Marcos Peralta. "Building Consumer Trust Online." Communications of the ACM 42.2 (April 1999): 80-85.

"ITL Bulletin." Information Technology Laboratory at National Institute of Standards and Technology. February 1998. http://www.nist.gov/itl/lab/bulletns/archives/98feb.htm. Accessed July 1, 1999.

Khare, Rohit and Adam Rifkin. "Weaving a Web of Trust." World Wide Web Journal 2 (Summer 1997). http://www.w3journal.com/7/s3.rifkin.wrap.htm.

Kini, Anil and Joobin Choobineh. "Trust in Electronic Commerce: Definition and Theoretical Considerations." Proceedings of the 31st Hawaii International Conference on System Sciences Jan. 6-9, 1998. Kohala Coast, HI: IEEE Computer Society, 1998.

Kramer, Roderick M. "Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions." Annual Review of Psychology 50(1999): 569-598.

Lasch, Erin. "Do you trust the Web?" Ohio CPA Journal 57 (Oct. 1, 1998): 8.

Luhmann, Niklas. "Trust: A Mechanism For the Reduction of Social Complexity." Trust and Power: Two works by Niklas Luhmann. New York: John Wiley & Sons, 1979. 1-103.

Moskowitz, Robert. "Ask Yourself: In Whom Can you Really Trust?" Network Computing 15 Jun. 1998: 33.

Nissenbaum, Helen. «The Meaning of Anonymity in an Information Age.» The Information Society 15:2 (1999):141-44

Petit, Philip. "The Cunning of Trust." Philosophy and Public Affairs 24 (Summer 1995): 202-225.

Posner, Richard. "The Right of Privacy." Georgia Law Review 12.3 (Spring 1978): 393-428.

Putnam, Robert D. Making Democracy Work: Civic Traditions in Modern Italy. Princeton: Princeton University Press, 1993.

Ratnasingham, Pauline. "Implicit Trust Levels in EDI Security." "Affording Digital Certificates and PKI Implementations." Journal of Internet Security 2 (January 1999): http://www.csci.ca/jisec/1999-03.htm.

Reiman, Jim. "In Web We Trust: Electronic Commerce." Direct 11(April 1998): 53.

Reiter, Michael K. "Distributing Trust with the Rampart Toolkit." Communications of the ACM 39 (April 1996): 71-74.

Renn, Ortwin and Debra Levine. "Credibility and Trust in Risk Communication." Communicating Risks to the Public. Ed. R.E. Kasperson and P.J.M Stallen. Dordrecht: Kluwer Academic Publishers, 1991. 175-218.

Salnoske, Karl. "Building Trust in Electronic Commerce." Business Credit 100 (Jan. 1998): 24.

Schneider, Fred, et al. Trust in Cyberspace. Washington D.C.: National Academy Press, 1999.

Schneider, Fred, et al. "Information Systems' Trustworthiness Policy

Context." Computer Science and Telecommunications Board project proposal for Information Systems Trustworthiness 1997. Online. 2 June, 1999. [http://www4.nas.edu/cpsma/cstbweb.nsf/86e5876b3bf8be848525631f00688fc5/ba2672794eca40cf852563300062ed26?OpenDocument]

"Security and Trust on the 'Net." IBM Vault Registry. Online. 1 June 1999. [http://www.software.ibm.com/security/registry/about/security.html]

Seligman, Adam. The Problem of Trust. Princeton: Princeton University Press, 1997.

Slovic, Paul. "Perceived Risk, Trust, and Democracy." Risk Analysis 13.6 (1993): 675-681

Steinauer, Dennis, Wakid, Shukri A., and Stanley Rasberry. "Trust and Traceability in Electronic Commerce." Standard View 5.3 (Sept. 1997): 118-124.

United States. "Violent Crime" Bureau of Justice Statistics: Selected Findings U.S. Department of Justice. April 1994, NCJ-147486

Wallace, Kathleen. «Anonymity.» Ethics and Information Technology 1:1 (1111):23-25

Weinstock, Daniel M. "Building Trust in Divided Societies." Political Philosophy 7 (1999): 263-283.

Woolford, David. "Electronic Commerce: It's All a Matter of Trust." Computing Canada 25 (May 7, 1999): 13.