“I’m on my way home, dear:” the role of plausible deniability in information systems and its impact on infosec practice

2nd Author
2nd author's affiliation
1st line of address
2nd line of address
Telephone number, incl. country code
2nd E-mail

ABSTRACT
In this paper, we describe the need for plausible deniability in everyday social relations. We are specifically concerned with everyday practice of plausible deniability in information systems and not in the mathematical models associated with untraceable communications and steganography. We provide two examples of technologies that require deniability for different purposes, and characterize deniability in terms of interpretation, knowledge, oversight and interpersonal relations. We further describe the implications of deniability on information security orthodoxy, by discussing how this pervasive social practice impacts the design of novel technology, the evaluation standards used for IT systems products, and the management of information security within organizations.

Categories and Subject Descriptors

General Terms
Design, Security, Human Factors.

Keywords
Keywords are your own designated keywords.

1. INTRODUCTION
In the past few years, both in the security and in the Human-Computer Interaction (HCI) communities, several authors have highlighted the importance of plausible deniability in social relations, and how it is enacted in technologically-mediated communication.

Notwithstanding this great amount of interest, there is still little research in technologies and mechanisms that explicitly support plausible deniability as part of their design. Often, plausible deniability is merely a byproduct of design choices, and is not sought intentionally.

In fact, deniability is at odds with traditional security principles such as accountability, responsibility and attribution. For example, the ITSEC (Information Technology Security Evaluation Criteria) defined information security as: “confidentiality, integrity and availability” [ITSEC]. At least two of these defining characteristics (integrity and availability) are in some way contrasting with the idea that individuals should be granted a certain amount of unaccountability within information systems. In order to achieve plausible denial, an individual may have to suggest interpretations of information which impact its integrity, and may have to reduce availability of certain information to others.

However, there is strong evidence that deniability may be an essential characteristic of successful communications technology. Studies in social psychology indicate that a substantial amount of *deception* is involved in everyday interactions [DePaulo]. Most of these practices that social psychologists bluntly define as deceptive, would not be frowned upon by most people. For example, people may “bend the truth” in order to conform to expectations, achieve social goals, or avoid unwanted or unpleasant consequences, as suggested by the title of this article. In fact, the practice is so pervasive that it may be more appropriate to avoid a term with negative connotation such as *deception* and instead talk about more neutral *social practices*.

Plausible deniability is an integral part of these social practices, because it affords the necessary leeway for individuals to engage in these practices without, or with reduced, fear of retribution [Walton]. In this sense, if social relations can be metaphorically likened to a machine, plausible deniability may represent its lubricant.

From a social standpoint, plausible deniability is not antithetic to the generation of trust—in fact, it actually enhances the opportunities for increasing interpersonal trust, but smoothing out irrelevant bumps while allowing individuals to concentrate their social efforts on the relevant disagreements. It benefits both parties involved, by allowing them to ignore issues which, if made explicit may require effort and time to resolve.

Plausible deniability also involves a *social* exercise, and is not merely the prerogative of an individual. It requires both sides to

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
Conference’04, Month 1–2, 2004, City, State, Country.
Copyright 2004 ACM 1-58113-000-0/00/0004…$5.00.

conform to a certain conduct, in which the party who is claiming deniability expects the other party to yield to the plausibility of his or her claims.

Plausible deniability is a concept deeply rooted not only in social relations, but also in judicial practice. We will not delve into the details of legal literature on plausible deniability, because it would bring the discussion too much out of scope. However, one may observe how the concept of *reasonable expectation of privacy* originating in the United States from the Forth Amendment (and compellingly described, in terms of the impact of modern technology, by the Supreme Court in Katz vs. US [Katz]) defines the practical bounds of plausible deniability.

In technologically mediated communication, achieving plausible deniability requires both parties to be comfortable with the use of the specific technology. There have been numerous accounts how cell phones are used for this purpose (see for example [Aoki]). In fact, the finely crafted affordances of cell phones[1] enable a social protocol that allows individuals sufficient leeway for claiming not having heard the phone ringing. Other successful communication tools also incorporate features that allow users to engage in plausible deniability practices (*e.g.*, Instant Messaging [Hancock]).

These authors show that plausible deniability is an important requirement for information technology, especially for artifacts meant to support communication amongst individuals. It is however difficult to design for deniability in practice, because the very concept represents a departure from established security policy and functions, both from a technical standpoint and an organizational one. On the other hand, compelling evidence suggests that it is a fundamental social need and that ignoring it can very well cause acceptance problems, can contribute to unwanted side effects (such as organizational sclerosis), or outright rejection of the technology.

For these reason, we think it is due time that the security community acknowledges the need for deniability and embeds this concept in the design, evaluation and management of information technologies. The remainder of the paper is organized as follows. In section 2, we describe some of the related work around the concept of plausible deniability and how it has been approached by sociologists, social psychologists, political scientists and information security researchers. In section 3, we describe two different applications which expose plausible deniability dynamics and needs. In Section 4, we indicate how plausible deniability can be characterized and in section 5 we suggest the consequences of such characterization on system design, IT evaluation and infosec management.

[1] As an example, consider just the process involved in answering to a phone call. When somebody calls, the phone discreetly whirrs or flashes and shows the calling number or name on the display. If the owner is driving, or in a meeting, he or she might well not even hear the vibration, or suffer only a brief distraction, and safely ignore the call, knowing that the call will be diverted to the voicemail system. Response in this case is delayed. The user can also check the phone number on the display and answer (or not) accordingly. One might also communicate to the other side one's unavailability by diverting the call immediately to voicemail without letting the phone ring further. Affordances are carefully crafted. The number of rings before activating voicemail (4 in many cases) allows for three-way response (answer, close the connection or ignore the call), and allows two-stage communication patterns back to the caller (request for attention, denial/acceptance by the called user, actual delivery of information by the caller).

2. RELATED WORK

In his 1975 seminal book *The Environment and Social Behavior*, Altman characterizes the process of creating privacy as a boundary setting process [Altman]. This process involves territorial behavior in the effort of creating a personal space and adjusting its boundaries dynamically, based on the needs of the moment. The relationship between plausible deniability and privacy is two-edged. On the one hand, a certain degree of privacy is necessary to enable credible denial in a social setting. On the other, plausible denial can be used to create the conditions under which the individual can be carve out his or her personal space.

Palen & Dourish have compellingly translated this boundary setting process into terms applicable to current information technology [Palen], and specifically cite plausible deniability as imperiled by the perpetual storage of individuals' personal information (such as writings or pictures) on an ever-expanding information network that allows anybody easy access and search.

Plausible deniability is typical of verbal communication practices and may involve deception in various forms. Walton describes plausible deniability in terms of public discourse, and links it to the evasion of burden of proof by the party claiming deniability. His account is rather negative, as it deals mainly with the consequences of libel and unsubstantiated anonymous claims by the press.

More positive characterizations of deniability spur from ethnographic studies of the communication patterns among both adults and teens. DePaulo *et al.* engaged in an extensive diary study to pinpoint the degree, reason and effects of deception in everyday communication [DePaulo], in which deniability plays an important role. Other studies have specifically targeted the teen-parent relationship [Jensen, Knox] and characterize lying in these relationships as a necessary component of the creation of self-identity in teens and of the ensuing separation process from the parents. Other studies involving the use of mobile telecommunication technologies by teens in Japan and Norway [Ito, Ling] stress the importance of the qualities of tool like text messaging, which allow hidden interaction (e.g. writing text messages is possible in situations which are tightly controlled) and also decouple interaction in the temporal dimension allowing for more leeway in structuring communication.

The theme of deception in mediated communication has recently received much attention in the Human Factors community. An article by Hancock *et al.* [Hancock] has investigated the use of deception in instant messaging, as opposed to email and voice communications, and has linked the amount of deception to the type of medium, explaining differences based on the qualities of the medium itself (*e.g.*, email is stored and thus affords less deception for fear of being caught)

Aoki and Woodruff describe the process of plausible deniability as that of making place for stories, and suggest how specific properties of imperfect technologies such as cell phones afford interactional ambiguity. They stress the importance of these imperfect technologies, another concept alien from the traditional security perspective that is focused on guaranteeing the best level of integ-

rity. Interactional ambiguity is a concept very similar to plausible deniability, as it implies a high degree of shared knowledge and intentional forgoing by one of the parties.

In the security literature, plausible deniability has received attention, especially in relation to the discussion of anonymity and unobservability. Chaum's idea of untraceable electronic mail using Mix networks allows parties to communicate not only unknown to third parties, but potentially also to one another [Chaum]. World-Wide-Web Mix networks have been implemented commercially for a brief period of time and allowed individuals to surf web sites while preserving plausible deniability of their actions.

One of the driving motivations behind the idea of Multilateral Security [Rannenberg] is that of allowing individuals to use telecommunication services without having to account for it (*e.g.*, for accessing counseling services carrying social stigma) [Müller]. Various techniques have been proposed for this purpose, including Mix networks for ISDN [Pfizmann].

Plausible deniability is also one of the reasons driving research in steganography, as some steganographic techniques allow to hide encrypted (pseudorandom) text into chaffing messages that are difficult for an attacker to prove constituting an actual encrypted message [Chapman].

The work in the security community has approached the issue of plausible deniability from a mathematical standpoint, striving to provide strong proofs that a certain communication mechanism or algorithm makes it unfeasible to trace a communication back to its owner. This aspiration for total unaccountability might however be politically impractical (considering current regulation governing telecommunication services wiretapping), too costly (given the impact of the organizational practices necessary to complement strong technical security functions), and ultimately unnecessary.

In this article we espouse however a different approach to plausible deniability, which is more attuned to the majority of day-to-day, benign social interaction. This approach views information security fundamentally as a risk reduction exercise, in which the cost of access to information or of its misuse can act as practical deterrents in most cases (similar in spirit to Povey's concept of optimistic security [Povey]).

3. EXAMPLES

In this section we briefly describe two example applications we have had the chance to observe during development in two institutions we have worked at. We will concentrate on the specific aspects related to plausible deniability. The first example relates to the use of digital videorecording technology in classrooms for supporting behavioral interventions with children with learning disabilities [anonymized reference]. The second example is a location-enhanced messaging system which has been the subject of a specific deployment study regarding plausible deniability of location disclosure [anonymized reference].

Besides providing a source for requirements and grounding in real-world experience, we hope to convey also the message that plausible deniability is very tightly related to information security, both because it needs security functions to be achieved and because it impacts the security of the people using the technology.

3.1 Example 1: Classroom Recording

Videorecording technologies in classrooms have been proposed several years ago for aiding intervention therapy with children with learning disabilities [Guidry]. Videos can be very helpful both as a therapeutic support (*e.g.*, observing children's behavior in class so that professional therapists do not need to follow each child in person—therapists are often a scarce and expensive resource), as communication tool (*e.g.*, with parents) and as training material for new therapists. However, one problems of video is that it requires much time for post-processing in order to be useful, and a dedicated operator which can operate the equipment.

For this reason researchers have proposed systems that automatically record classroom experiences, and allow simple tagging mechanisms (*e.g.*, when the teacher thinks something of interest has happened) to index the data for further retrieval [anonymized reference]. However, constant recording in classrooms hits against strong resistance form a multiplicity of sources, many related in some way to the concept of plausible deniability.

First, teachers (who are the first-level administrators of day-to-day behavioral interventions in many cases) often adopt *closed door* policies which do not allow the presence of third parties in the classroom during class. More than a form of hedging for fear of criticism, teachers point out that their resistance derives from a defense of **professional independence**, both as a matter of principle and of dignity (one teacher we talked with mentioned that especially *well respected* teachers may be most adamant about this independence). Teacher may want to avoid having parts of recording be taken out of context, thus influencing their perceived performance.

Second, parents (both of the children subject to intervention and of the others in the inclusive classroom) may be concerned with how their **children** will **appear** in videos, and often wish to retain both editorial and dissemination control on the produced material. In most cases parents may actually be more than willing to allow use of the videos, especially if the child is portrayed in a non negative light.

Third, school administrators seek protection against **liability risks**. Liability risks vary widely within regions in the United States, as some parts of the country have statistically higher rates of claims brought onto the educational system for alleged malpractice. For this reason, administrators as well as professional therapists (who are often dispatched to specific cases on a need basis) resist having recorded evidence that might be subpoenaed for this purpose.

All three these concerns are at least partially induced by a desire for plausible deniability. In the case of teachers and administrators one might argue that these concerns includes not having to account for each and every mishap that may happen in the school and avoid consequences for minor incidents or instances that may be misrepresented. In the case of parents, the main concern is that of protecting the social appearance of their children (*i.e.*, plausibly projecting a favorable image of them).

Clearly, effective **oversight** does exist in these environments: individuals or entities within the organization can enforce specific codes or performance standards, and intervene in cases of actual malpractice, but many feel that the benefits of pervasive recording may not outweigh the loss of "contractual power" embodied in the current social arrangements within schools. Some therapists even

go as far as suggesting that the recording of video may be too dangerous in all but carefully planned settings. Whether justified or not, this kind of resistance can spell the failure of a specific technology if designers do not take into consideration stakeholders' concerns. For this reason, making plausible deniability a primary concern of the requirements analysis seems to be the only viable option for a successful deployment.

3.2 Example 2: Location-Enhanced Messaging Application

The second example is a location-enhanced messaging application, which allows the user to send location requests to others by using a regular cell phone. The application allows the other party to respond with a self-defined location. That is, the location is not a geographical coordinate as provided by GPS, but a label indicated by the user, such as "home" or "office". In order to streamline interaction, the application presents to the disclosing party only the labels that are nearby his or her current geographical location. However, only labels are transmitted to the requesting party. This feature is fundamental in achieving plausible deniability and sets this system apart from other similar location-based services such as AT&T Find People Nearby.

The design and development process that led to this application is detailed elsewhere [anonymous reference]. We concentrate here only on the aspects relating to plausible deniability. Based on available literature, which is in part cited above, on the use of computer-mediated communication within plausible deniability practices, we decided to evaluate whether the application would support plausible deniability [anonymized reference] during a 2-week deployment with 11 participants (2 families with teenage kids).

Cases of outright deception about location occurred relatively rarely during the deployment; however, participants in our studies indicated that in those instances having the option to deny their actual location would have been quite important. Our participants affirmed that they would lie about their location in order to **preserve their individual privacy**, or as a way of **achieving positive, longer-term, social effects** (e.g., not telling the wife while at a particular store before Christmas). Participants who felt a need to deceive demonstrated the ability to do so with our application (by manipulating place names and outgoing messages).

Participants by and large rejected an "automatic reply" feature we had offered as part of the design (by enabling this feature, the phone would automatically respond to other's location requests). The main justification was the fear of loss of control over disclosures and the risk of confounding the receiving party with inaccurate disclosures.

Thus, the expressive freedom that the users of the application had for indicating their location allowed for sufficient level of plausible deniability. As a side note, in a antecedent study participants were asked whether a hierarchical modulation of location precision would have served the purpose of plausible deniability (*i.e.*, indicating the city instead of the street name). Participants overwhelmingly indicated that they would not have used this kind of "fuzzying" for maintaining their privacy. This suggests that the practices involved in plausible deniability may not be properly supported by naïve assumptions about varying degrees of location precision (state, city…) but may require more nuanced responses (such as ignoring requests, skirting questions by replying "busy" or with other evasive answers).

In this case, **oversight** may be provided by the telecom operators who may be in the position of preventing abuse, as with any other telecommunication service transported on their network.

4. CHARACTERISTICS OF PLAUSIBLE DENIAL

In the light of the two examples reported above, we discuss now characteristics of plausible deniability which we think have the greatest impact on the information security practice as discussed further below.

4.1 Ambiguous Interpretation

First, plausible deniability implies that a certain event or piece of information be open to multiple interpretations. This is compellingly described by Aoki and Woodruff [Aoki] in relation to the process of answering a cell phone.

In the case of location disclosures above, a "busy" message or ignoring a reply might both indicate that the recipient of the request is busy. However, the first reply provides an acknowledgement of the state of the exchange to the requesting party, whereas simply ignoring a request leaves the other party with the doubt of whether the message was delivered, viewed and a decision was made not to answer. Clearly, the two cases prompt different interpretations, and different social consequences.

In the case of the classroom recording, we mentioned the risk of malpractice suits brought on to schools. Clearly, interpretation of actual events is greatly impacted by the presence of rich data (video recordings). If video recordings are available, and obtained legally, they may be used in legal proceedings and unbalance plausible deniability, regardless of their incorrect interpretation if they are taken out of their original context.

4.2 Lacking Knowledge

Different interpretations are as much a function of selection of evidence as they are a product of ambiguous or lacking knowledge. In order to achieve actions that can be interpreted in different ways, designers can make specific security functions and architectural choices. For example, in the mobile location disclosure tool described above, the very content of the delivered messages lends itself to ambiguous interpretations that leave space for subsequent denying their content. For example, in the deployment study for that application, instead of replying with the name of a certain shopping mall, one participant told one family member that he was "running errands" as a way of avoiding questioning regarding Christmas gifts.

Of course, architectural qualities of the technology must support the generation and propagation of this kind of ambiguous knowledge. Unobservability of actions (as defined in the multilateral security literature) enables plausible deniability of actions. Confidentiality is required to maintain the segmentation of communication that enables plausible deniability of specific information, such as someone's location.

4.3 Oversight Structure

Oversight is fundamental to the plausible deniability construct. Without oversight against abuse, the system may break down and plausible denial may quickly degenerate in mistrust. For example,

when discussing the first example, rejection of video recording in classrooms is only possible given that teachers are trusted of not abusing their unaccountability, and other oversight methods are available.

Likewise, while occasional denial may pass unnoticed, persistent lying by a teenager to the parents about his or her location may carry strong negative consequences. In extreme cases, location information can be sought directly from the operator, as has happened in a number of cases in which cell-id transaction records have been used to trace the movements of alleged criminals.

Resorting to oversight functions carries often a high cost which may be warranted only in specific circumstances (*e.g.*, the subpoena or warrant needed for accessing location information from an operator). This balancing ensures that plausible deniability practice conform within a range of socially accepted behaviors: in ordinary circumstances, the person claiming deniability can rest assured that his or her "deviations" will not be uncovered, while exceptional circumstances may still be prosecuted.[2]

4.4 Interpersonal Relations

Plausible deniability is largely an interpersonal practice, as suggested by the surveyed literature. This is due to several interrelated reasons, whose discussion is not in the scope of the present article. By contrast, inter-organizational relations are often structured regulated by contracts, case law and legislation at the level that concerns us (i.e. information technology security). For example consider the Sarbanes Oxley Act in the United States [USC2] which vastly increased accountability requirements for publicly traded companies.

This is clearly manifested in the second example above. Even in the first example, plausible deniability really relates to situations in which the party claiming deniability is an individual, even if an organization may take his or her defense as a matter of responsibility (*e.g.*, in the case of a malpractice suite against the school system, centered on a specific teacher).

This observation provides a good structuring tool for system analysis: in all information systems where individuals are involved attention should be given to plausible deniability.

However, it should be noted that *within* organizations, individuals still have a need for plausible deniability. If IT systems mediate relations or engender practices between the organization and an individual that is in some form subject to the organization, deniability should be accounted for (see below: information security management).

5. IMPACT ON INFORMATION SECURITY PRACTICE

We have described two salient case studies that show what are the plausible deniability concerns of users of information technologies in very different settings and we have subsequently characterized the concept of plausible deniability in this context. Now, we will discuss the impact of each of these characteristics on four aspects of information security: the design of technology, evaluation and certification standards, information security management and regulatory intervention.

[2] This interpretation conforms to our view of information security as balancing risk and cost.

5.1 Technology Design

Over the years, the security community has devolved much efforts in building increasingly sophisticated access control systems, encryption mechanisms and network security tools. However, from the HCI literature we know that technology is used by people in ways often unforeseen by the developers [Grinter] and that in order to create truly secure systems understanding is necessary of how they are used in practice [Zurko]. We would like to highlight the role of design features that have an impact on users' security but are not strictly speaking security functions.

For example, in the mobile location-enhanced messaging application described above, the ability of sending place names instead of geographical coordinates may not be technically a security feature. Nevertheless, it has a strong impact on the users' security: not only it allows the user to plausibly deny his or her presence at a certain location as part of everyday social interaction with trusted friends, but it also helps protect the actual physical security of the user in the case of requests by individuals impersonating some friend, as it discloses a name that in most cases is not easily traceable to a physical location, without knowledge of the customs and habits of the disclosing party.

In this case, what provides the security property is not an access control system but simply flexibility in the formulation of a reply message. The flexibility in defining the label introduces a level of ambiguity in the interpretation of the reply which leverages off partial knowledge.

There are other ways of introducing **ambiguity** as part of a technical design. For example, Hong *et al.* discuss the privacy features of Confab, a system for the automatic management of personal *context* information for ubiquitous computing (in the ubiquitous computing domain, "context" refers to incidental information regarding a user or system, such as his or its location) [Hong]. In that system the default (unless otherwise authorized) response to any query for personal information is "unknown," whether it exists or not. This introduces ambiguity in the design of the system, thus enhancing the ability to plausibly deny the user's context.

The need for **oversight** structures, from the technical standpoint, translates in the presence of some kind of Trusted Third Party (TTP). The specific enactment of these TTP entities is left unspecified, but invoking their functions should be commensurate to the effects of the abuse of plausible deniability. In the case of the cell-phone based messaging application the TTP may be the telecom operator. In the Confab system described above the TTP may be the context service provider.

As mentioned above, the **interpersonal** nature of plausible deniability should be accounted for. Successful messaging systems support various degrees of plausible deniability and are adopted for different uses also based on how difficult it is to achieve deniability in practice (compare the type of conversation happening through email vs. on the phone [Hancock]). Security requirements analysts should account for these differences and qualities in all designs that support some form of communication among individuals

Summarizing, we offer the following suggestions as ways to account for plausible deniability into information systems:

– consider all aspects of design with security implications, not just narrowly defined security functions;

– built, into interpersonal communication tools, provisions for plausible deniability. Example of such provisions are: increasing ambiguity in the information managed by the system (*e.g.*, by providing multiple alternatives for a specific information item); leaving more control on disclosed information to users; and, in case of doubt, disclosing less specific, rather than more specific, information.

– identify and correctly price access to redress or oversight mechanisms to avoid abuse of plausible deniability.

5.2 Security Evaluation and Certification Standards

Although the limited market success of the Common Criteria and other IT security evaluation and certification standards may cause to question their future use as normative instruments, we think it is important, due to their strong influence on the security community, to highlight how supporting plausible deniability in communications might impact these instruments.

The Common Criteria (CC) include a Privacy Class (quite innovative for this kind of standards originating from military security requirements), which includes functional requirements addressing the areas of anonymity, pseudonymity, unlikability, and unobservability [ISO15408]. For example, the anonymity functional requirement (FPR_ANO.2) may allow to specify that a web server must protect its users by avoiding the collection of their IP addresses during accesses to the website.

However, we have seen that there is more to plausible deniability than the ability of sending anonymous messages. The Common Criteria are ill fit to describe more complex relations between the users of the system. For example, it may require complex fiddling with access control requirements to describe a requirement such as: "only location labels and not actual geographical coordinates are transmitted between users of the system."[3]

Adding requirements that guarantee that certain information within the system may be subject to **ambiguous interpretation** may be even more complicated. In fact, one of the stated principal goals of the CC is that of assuring *information integrity*. **Oversight** structures in the form of TTPs are really not foreseen by the CC: the standard still endorses a monolithic view of the system where users, administrators and owners share the same goals and are governed within the same organizational structure.

All in all, security evaluation and certification standards, such as the Common Criteria [ISO15408], only consider security functions as part of the application requirements under review during an evaluation as part of the Protection Profile / Security Target documentation. Other features which may have a strong effect on user security are ignored by these standards. Thus, as information technology will be used in more diverse and pervasive settings, the Common Criteria risk becoming increasingly marginalized as evaluation systems because they fail to address the real issues of concern to the users.

One possible option for addressing these concerns is that of expanding the Common Criteria to address more "high level" security requirements, either through custom additions to the standard, or as part of a future, more flexible standard.

5.3 Information Security Management

Within the domain of information security management, (criminal) liability concerns may curtail the application of the following suggestions for recognizing plausible deniability as part of organizational structure. Information management within commercial and government organizations is increasingly regulated by legislation, such as data protection legislation like HIPAA [USC1], financial transparency laws such as the Sarbanes-Oxley Act [USC2] and information security regulation such as FISMA [USC3].

However, there are still many cases in which the above suggestions may be applied.

Consider the case in which employees use of computing systems for purposes unrelated to their occupation, especially for information services that cater to **interpersonal needs**. This is a practice often tacitly allowed in organizations, where workplace discipline and organizational sensibility allow it. However, rarely do infosec policies within organizations acknowledge these practices. International Standard 17799 does not even contemplate the personal use of information systems, which might have significant impact on security [ISO17799]. In fact, that standard endorses close monitoring of user information systems for the purpose of detecting misuse. Complete logging of all user activity eliminates **ambiguity** and curtails the ability of engaging in plausible deniability practices even for activities which may as well be harmless and are, as we have seen, necessary for conducting healthy everyday social interaction.

Organizational policies supporting plausible deniability in this case would include provisions for avoiding or restricting the logging of the activity of individual users within the information system (such as instant messaging for personal purposes).

Oversight functions may still be part of the policy (such as enabling logging in specific circumstances), but special authorization may be required to enact these functions, in order to heighten the cost of accessing them and preserving limited unaccountability.

One way of introducing plausible deniability as an acknowledged and regulated part of organizational security policy would be to create a two-tier management system. At the lower tier, some activities such as the personal use of computing systems may be explicitly allowed. This would codify institutionalized practice, thus avoiding the dangerous situation in which official policy is not representative of actual organizational behavior. At the second level, this kind of policy would still retain the option of enforcing regulation, in extreme cases of abuse, in which the cost of accessing the oversight functions (*e.g.*, obtaining an authorization from an executive) would be commensurate to the potential damage caused by misuse.

6. CONCLUSIONS

Information security research has by and large ignored the social need for plausible deniability. The mathematical formulations of the concept proposed by research in untraceable messaging and steganography really do not reflect the ways people engage in this practice in everyday life.

[3] Similar problems with the expressive power of the Common Criteria were exposed in previous work attempting to specify Protection Profiles for remailer mixes. [anonymous reference]

The result is a potentially dangerous mismatch between expectations of security of products and organizations and their actual use and behavior in everyday life.

Based on our research on applications of information technology with significant end-user privacy and security concerns, and with the help of two example applications which underwent significant requirements analysis and development, we characterize the social practice of plausible deniability in a way that can be applied to information security research at three distinct levels: during design of novel technology, during its evaluation, and during management.

Specifically, we invite, with documented arguments, researchers and practitioners to:

- consider all aspects of design with implications on interpersonal communication, not just narrowly defined security functions, as part of the analysis of security requirements;
- explicitly built, into interpersonal communication tools, provisions for plausible deniability;
- explicitly plan, *and price adequately*, the access to redress or oversight mechanisms to avoid abuse of plausible deniability;
- expand evaluation standards such as the Common Criteria to address higher level security requirements that are relevant to the users;
- introduce plausible deniability in information security management practices, *e.g.*, by employing two-tier management structures.

We think that this shift in priorities for the security community will be necessary in order to continue catering to the needs of the inhabitants of a society increasing permeated and mediated by information technology.

7. ACKNOWLEDGMENTS

To be completed upon acceptance.

8. REFERENCES

[Altman] Altman, I., (1975), The Environment and Social Behavior—Privacy, Personal Space, Territory, Crowding, Brooks/Cole Publishing Company, Monterey, CA. ISBN 0-8185-0168-5.

[Aoki] Aoki, P.M., Woodruff, A.: Making Space for Stories: Ambiguity in the Design of Personal Communication Systems, in Proc. CHI 2005, Portland, OR, USA: ACM Press, 181–190.

[Chapman] Chapman, M., Davida, G: Plausible Deniability Using Automated Linguistic Stegonagraphy, Davida, G., Frankel, Y., Rees O. (Eds.): InfraSec 2002, LNCS 2437, pp. 276–287, 2002. Springer-Verlag

[Chaum] Chaum, D. Untraceable electronic mail, return addresses and pseudonyms. CACM 24:2 (1981), 84-88.

[DePaulo] DePaulo B.M., Kashy D.A.: Everyday Lies in Close and Casual Relationships Journal of Personality and Social Psychology. Vol. 74 (1) January 1998, pp. 63–79. American Psychological Association

[Grinter] Grinter, R., Dourish, P., Delgado de la Flor, J., Joseph, M., Security in the wild: user strategies for managing security as an everyday, practical problem, Personal and Ubiquitous Computing archive, Volume 8, Issue 6 (November 2004), 391 - 401

[Guidry] Guidry, J., van den Pol, R., (1996) Augmenting Traditional Assessment And Information: The Videoshare Model, Topics in Early Childhood Special Education, March 1, 1996, Vol. 16, Issue 1

[Hancock] Hancock, J.T., Thom-Santelli, J., Ritchie T.: Deception and Design: The Impact of Communication Technology on Lying Behavior, in Proc. CHI 2004, Vienna, Austria: ACM Press

[Hong] Jason I. Hong , James A. Landay, An architecture for privacy-sensitive ubiquitous computing, Proceedings of the 2nd international conference on Mobile systems, applications, and services, June 06-09, 2004, Boston, MA, USA

[Ito] Ito, M. and Daisuke, O.: Mobile Phones, Japanese Youth and the Replacement of Social Contact, in Ling, R. and Pedersen, P. (eds) Front Stage/Back Stage: Mobile communication and the Renegotiation of the Social Sphere, Conference Proceedings, 22-24 June 2003, Grimstad, Norway.

[ISO15408] International Organization for Standardization, ISO/IEC 15408:1999 (Parts 1-3) Information technology – Security techniques – Evaluation criteria for IT security, 1999, available at: http://www.commoncriteriaportal.org, last visited 4/10/2005.

[ISO17799] International Organization for Standardization, ISO/IEC 17799:2000 Information technology – Code of practice for information security management, 2000.

[ITSEC] Information Technology Security Evaluation Criteria, June 1991, Version 1.2.

[Jensen] Jensen, L., Jensen, J., Feldman, S., Cauffman, E.: The Right to Do Wrong: Lying to Parents Among Adolescents and Emerging Adults, Journal of Youth and Adolescence, Vol. 33, No. 2, April 2004, pp. 101–112 (2004)

[Katz] Katz v. United States, 389 U.S. 347; 88 S. Ct. 507 (1967)

[Knox] Knox D., Zusman, M.E., McGinty, K., Gescheidler, J.: Deception of Parents During Adolescence, Adolescence, Vol. 36, No. 143, Fall 2001, Libra Publishers, San Diego, CA

[Ling] Ling, R., Norwegian teens, mobile telephony and SMS use in school, Technical Report Telenor R&D N 7/2000 (2000)

[Müller] Müller, G. and Rannenberg, K., Eds. (1999). Multilateral Security in Communications, Volume 3: Technology, Infrastructure, Economy, Addison Wesley, ISBN 3-8273-1426-7

[Palen] Palen, L., Dourish P. (2003). Unpacking "Privacy" for a Networked World, in Proceedings of CHI 2003, ACM Press

[Pfizmann] Pfizmann, A., Pfizmann, B., Waidner, M., ISDN-MIXes: Untraceable Communication with Small Bandwidth Overhead, Informatik-Fachberichte; Vol. 267, Kommunikation in Verteilten Systemen, Grundlagen, Anwendungen, Betrieb, GI/ITG-Fachtagung (1991) 451 - 463

[Povey] Povey, D.: Optimistic Security: A New Access Control Paradigm. Proc. New Security Paradigms Workshop. 1999. Ontario, Canada: ACM Press

[Rannenberg] Rannenberg, K. Multilateral Security: A Concept and Examples for Balanced Security. Proc. 2000 New Security Paradigms Workshop, ACM Press (2001), 151–162

[USC1] 42 USC 1320 et seq. (United States Health Insurance Accountability and Portability Act of 1996)

[USC2] 18 USC 1514A et seq. (Sarbanes-Oxley Act of 2002)

[USC3] 44 USC 3541 et seq. (Federal Information Security Management Act of 2002)

[Walton] Walton, D., Plausible Deniability and Evasion of Burden of Proof , Argumentation 10: 47-58, 1996. Kluwer Academic Publishers.

[Zurko] Zurko, M.E. Simon, R.T., User-centered security, Proceedings of the 1996 workshop on New security paradigms, p.27-33, September 17-20, 1996, Lake Arrowhead, California, United States