
Secrets and Lies in Computer-Mediated Interaction: Theory, Methods and Design

Adam N. Joinson

School of Management,
University of Bath
Bath
BA1 7AY
A.Joinson@bath.ac.uk

Jeffrey Hancock

Department of Communication
Cornell University
320 Kennedy Hall
Ithaca, NY, 14850
jth34@cornell.edu

Pam Briggs

School of Psychology and Sports
Science
Northumbria University
City Campus
Newcastle upon Tyne
NE1 8ST
p.briggs@unn.ac.uk

Abstract

The keeping of secrets and practicing of deception are commonplace in everyday social interaction. They also serve an important role in encouraging social cohesion. However, for HCI practitioners, the challenge is to design systems that enable exactly this kind of flexibility and ambiguity in social behavior while also maintaining trust and authenticity. This workshop will bring together researchers of both deception and secrecy in computer-mediated interaction, alongside designers of systems, to face up to these challenges and develop a road map for the future. The workshop will act as a venue for the synthesis of theory with design, and propose ways to face the challenges of enabling authentic social interaction in computerized environments.

ACM Classification Keywords

H.5.2. Information interfaces and presentation (e.g., HCI): User Interfaces, Evaluation/methodology

Keywords

Deception, Secrecy, Privacy, Design, Security

Introduction

New communication technology often raises concerns about the authenticity of users' utterances. The use of

Copyright is held by the author/owner(s).
CHI 2008, April 5–10, 2008, Florence, Italy.
ACM 978-1-60558-012-8/08/04.

wax seals in written communication was a signal that the authorship was genuine [7]. The early development of the telephone was characterized by concerns over the honesty of communication without face-to-face interaction [5]. Similar concerns have been raised regarding computer-mediated interaction – both in terms of human-to-human interaction and people’s dealings with computerized systems. For instance, Phishing [3] relies on the ability to misrepresent via computer interaction in order to extract financial gain. Online dating profiles rarely match exactly the person seeking a date, instead positively skewing the description in the posters’ favor [4].

Simultaneously, computer-mediated interaction also reduces the likelihood that people will be able to keep aspects of their lives secret. The combined effects of ubiquity, mass (and cheap) storage, linked databases and - in an increasingly security-conscious world - the collection of personal data for authentication or personalization [11] means that for many people, their privacy is eroded in ways unimaginable in the past. Paradoxically though, people seem to be more willing to disclose intimate aspects of their lives via computer-mediated interaction compared to, say, face-to-face [6]. This ‘strangers on the Internet’ phenomenon has been identified in numerous studies [5; 6], and suggests that, when online, secrets are the last thing on people’s mind.

Secrets and lies in computer-mediated interaction have close links to other topics of particular interest to HCI practitioners, including issues of trust [10; 9], ambiguity in systems design [2], security [8] and privacy [6]. However, thus far there has been little progress towards a unifying model of secrets and lies in computer-mediated interaction.

Theory and Methods

A clear understanding of why people deceive and keep secrets in computer-mediated interaction, and when they choose to reveal intimate aspects of themselves, is central to the design of socially intelligent tools. Currently, our theoretical understanding of these different phenomena is limited, in part because researchers and practitioners have few forums in which to openly exchange ideas and experiences. The workshop will provide such an opportunity.

The methods used to study deception and secrecy / self-disclosure in an HCI context are similarly under-developed, and suffer from insularity. Current methods, including self-report questionnaires, ethnographic and diary methodology, and laboratory experiments, each have unique advantages and disadvantages in the study of secrets and lies. The workshop will provide an opportunity to investigate the variety of methods used to study secrets and lies in computer-mediated interaction, as well as encouraging the introduction and cross-fertilization of methods from different domains and disciplines.

Design Challenges for HCI practitioners

Issues of privacy and trust pose challenges for HCI practitioners that have been considered in detail in previous CHI papers and workshops [e.g., 1; 10]. The increases in social uses of computer-mediated interaction, alongside the development of ambient and ubiquitous technologies, make a fuller understanding of these topics of critical importance. The workshop on deception and secrecy builds on this earlier work, while also extending the scope to consider practical challenges for HCI practitioners. For instance, in many cases deception may be a valid response to a request. Take for

instance, a request from a line manager about an employee's location while they are off duty. While the employee might not wish to refuse the request, they might want not to be fully candid in their response. In wanting to keep their location *secret*, the employee might engage in outright deception ("I am in the hospital"), or might choose ambiguity to blur their location ("I am in the east-end of the city"). Deception may also act to encourage social cohesion, for instance, by smoothing social interaction and reducing disagreement.

The design of tools and systems that enable this kind of deception and secret keeping, while also enabling trustworthy, authentic interactions, is a central component of the workshop. The development of trust is one of the most important aspects of person-to-person interaction, which incorporates the ability to identify misrepresentation. Control over when we reveal personal information to others (or systems) may also form an important part of this trust building, as well as forming an important part of any security agenda. Increasingly, we will use tools to not only engage in person-to-person interaction, but also to make decisions on our behalf about the identity and intentions of those we interact with, and based on that, what we reveal about ourselves in return. The onus then, will shift to the design of tools, and methods for interacting with those tools (e.g. to set our preferences). The development of a unified theory of deception and secrecy in computer-mediated interaction is critical for the successful implementation of these technologies.

Key questions

The increasingly social nature of computer-mediated interaction poses unique challenges for HCI practitioners. Some of the key issues are:

- What theoretical models of deception and secrecy might be useful to the designer?
- Do people engage in higher levels of deception when engaged in computer-mediated interaction (CMI)? What motivates the choice of media for deceptive behavior, and how might CMI shape the nature of deceptions?
- What motivates people to keep secrets during CMI? When do we choose to reveal information?
- Does a unified model of deception and secrecy in CMI exist?
- How can deception and secrecy be best studied? What methods are available?
- What are the implications for the design of CMI systems? Do techniques for the reduction of deception impinge users' legitimate desire to keep secrets?
- What are the security implications of designing with deception and secrecy in mind?
- Can room for socially beneficial deception and secrecy be designed into systems? Or should designers simply leave it up to users to adapt systems to their own practices of deception and secrets?

Immediate and Long Term Workshop Goals

This workshop will bring together theorists and practitioners from HCI, Security and Privacy studies, CSCW, Ubiquitous and Ambient Technologies, and the

social sciences to discuss the integration of, and challenges posed by, deception and secrecy in computer-mediated interaction. The diverse group of participants offers the opportunity fruitful collaboration across disciplinary boundaries on a critical topic for HCI.

In the longer term, the aim of the workshop is to set out a road map for the integration of deception and secrecy into future technologies. Specifically, this road map will include scenarios, proposed requirements for design, implementation and behavior of technology, suggestions

for ways to combine users' desires with the need for privacy, trust and authentication, and ultimately, ways to allow people to control and reflect on the meaning of secrets and lies in their own lives and through the use of social technologies.

In light of the road map, the workshop will produce a draft outline of the key issues in the area, and methods to move these issues forwards. Workshop participants will be asked if they would like to submit full versions of their papers for future publication.

References

- [1] Aoki, P. & Woodruff, A. Making space for stories: Ambiguity in the design of personal communication systems. *Proc. CHI 2005*, AMC Press (2005). 181-190.
- [2] Boehner, K. & Hancock, J.T. (2006). Advancing ambiguity. *Proc. CHI 2006*, ACM Press (2006), 103-107.
- [3] Dhamija, R., Tygar, J.D., & Hearst, M. (2006). Why phishing works. *Proc. CHI 2006*, ACM Press (2006), 581-590.
- [4] Hancock, J.T., Toma, C., & Ellison, N. The truth about online dating. *Proc. CHI 2007*, ACM Press (2007), 449-452.
- [5] Joinson, A.N. *Understanding the Psychology of Internet Behaviour: Virtual Worlds, Real Lives*. Basingstoke: Palgrave Macmillan, 2003.
- [6] Joinson, A.N. & Paine, C.B. Self-Disclosure, Privacy and the Internet. In A.N. Joinson, K.Y.A McKenna, T. Postmes and U-D. Reips (Eds). *Oxford Handbook of*

Internet Psychology (pp. 237-252). Oxford University Press, 2007.

[7] Ong, W. J. *Orality and Literacy*. London: Methuen, 1982.

[8] Roth, V., Straub, T., & Richter, K. Security and usability engineering with particular attention to electronic mail. *International Journal of Human-Computer Studies*, 2005, 51-73.

[9] Riegelsberger, J., Sasse, M.A., & McCarthy, J.D. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies*, 62, 2005, 381-422.

[10] Sillence, E., Briggs, P., Fishwick, L., & Harris, P. Trust and mistrust of online health sites. *Proceeding CHI 2004*, ACM Press (2004), 663-670

[11] Sparck-Jones, K. Privacy: What's different now? *Interdisciplinary Science Reviews*, 28, 2003, p.287-292