Privacy Issues for the Disclosure of Emotions to Remote Acquaintances without Simultaneous Communication

Sébastien Duval[1], Christian Becker[2], Hiromichi Hashizume[1]

[1] National Institute of Informatics
Hitotsubashi 2-1-2, Chiyoda-ku, Tokyo-to 101-8430, Japan
{duval, has}@nii.ac.jp
[2] Artificial Intelligence Group, Faculty of Technology, University of Bielefeld
P.O. Box 10 01 31, 33501 Bielefeld, Germany
cbecker@techfak.uni-bielefeld.de

Abstract. We discuss the privacy issues related to the design of systems that disclose information about emotions to remote acquaintances, without simultaneous communication: users do not chat, see or hear each other. We consider the acquisition of information, storage, processing, multi-modal rendering, and interactions. We illustrate our points with the system we designed for affective bonding and support with family and friends. Our most significant contribution is the provision of a first overview of the whole process for everyday life uses.

Keywords: Communication, Emotions, Family, Friends, HCI, Privacy, Ubiquity, Wearable.

1 Introduction

Disclosure of emotions can strengthen affective bonds between acquaintances such as family members and friends. However it raises privacy issues for senders and recipients due to the acquisition, storage, and rendering of information. These issues must be considered to avoid negative side-effects, satisfy psychological needs, and foster the adoption of systems by the general public [1]. Finding ways to protect privacy while preserving useful affective services is most important because these services do not exist yet; opportunities will be limited when we have to deal with heterogeneous and legacy systems.

We consider here the case of disclosure to remote acquaintances, without simultaneous communication: users do not chat, see or hear each other. This scope is appropriate for continuous information about acquaintances living in different areas, for short (e.g. business trips) or long (e.g. studies abroad) periods. Disclosure face-to-face with, or within the vicinity of, acquaintances shall be treated ulteriorly, as well as simultaneous communication with devices like cellular phones and networked cameras.

We first present background information about emotions and privacy, then discuss the machine and human sides of the disclosure process, taking as example a system we developed for the family and friends. Finally we conclude with a discussion on global issues.

2 Background Information

We first define the scope we cover in the following sections, and then present a dedicated system, which we later use to illustrate our points.

2.1 Scope Covered

For the sake of clarity, we first define what we mean by *emotions* and *privacy*. Then we highlight the risks associated to the disclosure of emotions in the current context.

Emotions. Although the term *emotion* is frequently used, definitions tend to be circular. Even psychologists still disagree widely on its exact meaning:

> "[W]ere one to ask 'What is basic about emotions?,' one would surely get embroiled in controversy, both in terms of what is meant by 'basic' and what it means to be an 'emotion'.", Panksepp [2, p20].

For the kind of services we aim to create, we can be satisfied with a definition that corresponds to *feelings elicited briefly* (seconds, minutes) *by quick and/or unforeseeable antecedents* (e.g. a car accident as opposed to bad weather).

Privacy. Privacy is the state of being able to be alone, unobserved, free from public attention. More specifically, information privacy can be defined as 'the right to control the disclosure of and access to one's personal information' [3]. It covers the right to know and correct what a third party knows and provides about us, and even to restrict access to such information. This notably applies to raw data, videos and evaluations of emotional states.

Perspectives on Communication and Awareness. Disclosure of emotions can provide much information to recipients. Without additional data, causes cannot be deduced. However, with simultaneous communication or context awareness, inferences of recipients and third parties can become reliable. Table 1 describes the influence of networking, additional communication channels, and types of displays on risks regarding misunderstandings, leaks, and inferences.

Table 1. Impact of several settings on risks related to the disclosure of emotions.

	Misunderstandings	Leaks	Inferences
Remote service	-	Risky	Risky
Local service	-	Safe	Safe
Emotional information only	Risky	Safe	Safe
Simultaneous audio/video	Safe	Risky	Risky
During face-to-face contacts	Safe	Safe	Safe
Public display (wearable screen)	-	Risky	Risky
Private display (data-glasses)	-	Safe	Safe

2.2 Design of a System Dedicated to the Family and Friends

After introducing the goal of the system, we indicate its main features then present its visual interface.

Goal and Features. We designed a ubiquitous system to strengthen affective bonds and allow affective support for distant relationships with the family and friends [4]. To complement existing technologies and services, we considered sharing information about emotions. We proposed to acquire data from each user, process it on a server, and transmit personalized updates to acquaintances. In our design, emotion-related data is acquired from physiological sensors embedded in a personal wearable, and copies of e-mails received by the server from registered addresses. After processing the data, the server checks which users should get updates and accordingly creates updates based on the originator's and recipients' preferences. Personalization and privacy information are stored on the server.

Visual Interface. Information can be accessed on a web site (after identification), by e-mail, or on a wearable display that is continuously updated. Emotional states are displayed using a *soap bubble* metaphor (figure 1) in which the background color represents the state of the group, and colored bubbles the state of individuals. The speed of the upward flow reflects that of variations. *Current*, *Day*, and *Week* views are available. This interface works with touch-sensitive displays embedded in watches or sleeves, or semi-transparent glasses combined to mobile devices.

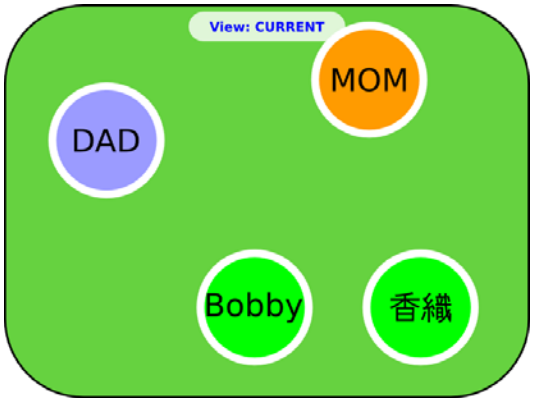

Fig. 1. Example of view for acquaintances' current state with the wearable interface.

This metaphor provides a good understanding of the system because it shows data as volatile (bubbles burst and vanish, data is retained for short periods only), because it reflects the passing of time, and because each bubble is independent but from the same source (individuals are from the same family or group of friends). It also allows users to hide meaning by freely associating colors and shapes to intensities and types of emotions.

3 Machine Side

The machine side of the disclosure process mainly deals with first phases: acquisition, transmission, storage, and processing of data.

3.1 Acquisition of Data and Information

Emotions can be evaluated by changes in subjective experience, behavior and physiology [2], and information can be provided to a computer system using introspection, human observers, or machines.

Acquisition by Humans. With introspection, a user indicates her sensations, feelings, and thoughts. This approach is potentially the most accurate because the user has the broadest and deepest access to relevant information. However, it is not perfect due to limited attention and subconscious processes. Observers can also feed systems with useful evaluations. They cannot access internal knowledge of the targeted users but can notice revealing physical behaviors; if trained or familiar, they can provide particularly insightful input. Input by humans is not realistic for continuous real-time services. However it can be used to e.g. inform a group of friends about the state of those met during the day.

Input by humans raises limited privacy issues because only partial, subjective, and eventually high-level information is provided (with possible mistakes or *lies*). One always has the possibility to deny observations or inferences.

Acquisition by Machines. Wearable computers and smart environments are particularly suitable to evaluate users' emotions. A wearable may acquire data about its user[1] with physiological sensors and multimedia analysis. Smart environments have limited access to bodily information (no physiological sensors available) but more resources and space. Thus they can comprise more sensors and process more data. Machines cannot access users' internal knowledge but, with enough time and databases, can be trained or become familiar with specific persons. Raw data can be extracted, timed, cross-checked, and analyzed in depth (later, with improved algorithms) for different purposes such as investigating a user's health, activities or beliefs. The (un-)reliability of current technologies and algorithms has little impact on our discussion because increasing reliability is expected due to innovations.

Systems should therefore be designed to acquire only required data, which means carefully selecting sensors, extracting only required information, and discarding the rest. Typical questions would then be: are physiological sensors required? Do we need precise evaluation of heartbeats or just speed gradients? Should we install standard or infrared cameras? In which rooms? Whenever possible, data should be preprocessed at the electronic/mechanic level before transmission to the computer, and transfers should be limited to minimal qualitative information.

---

1 When acquiring data about *other people*, wearables can be considered as smart environments.

Illustration with our System. Emotional data is currently acquired from physiological sensors and e-mails; it is then processed on a remote server. The system may be improved by adding a *personal* software agent residing in the wearable computer. The agent would select whether to read the sensors or e-mails depending on tasks, then process the data locally and transfer only high-level information. It would let users choose recipients and the accuracy/frequency of transmitted data. By default, raw data would not be sent.

3.2 Transmission, Storage and Processing

Whether with local or remote servers, data should be protected from unauthorized exploitation. Besides, users should keep control over accessible data.

Architecture, Algorithms, and Policies. Architectures and algorithms influence the requirements for processing, data retention, and encryption. Communication should be authenticated and encrypted to ensure that only selected acquaintances and trusted servers access the information. After a transmission, the sender and recipients should apply retention policies. With peer-to-peer (P2P) services, leak-related risks are limited. However retention policies are critical for centralized services: servers are easily identified and attractive targets that potentially store all data about every user. Finally, if learning is used to evaluate emotions, model-based algorithms should be favored over instance-based ones because mathematical models hide original data.

Although P2P architectures appear more respectful of privacy than centralized ones, the selection also depends on other constraints such as energy. For example, with P2P architectures, mobile devices would send duplicated messages (to each recipient). With centralized architectures data can be sent once then processed by servers, saving energy and making the service more viable for continuous use.

Whatever architecture is chosen, a standard retention policy would be to minimize data, store it with the largest granularity required, and remove it as soon as possible. If continuous real-time retrieval is unnecessary, a single–average–value can be retained per appropriate period. For asynchronous services data may need to be stored longer. The retention policy should be clear to users and, ideally, negotiable.

Control by Users. User's control over sent and stored information is critical. Because the modification of data undermines trust in systems [1], it should be avoided. Removal poses similar challenges: what becomes a "feeling of the day" after selective deletions? Tampered information is considered useless, and results in the rejection of systems [1]. Finally, deactivation functions are appreciated proactive solutions to potentially embarrassing or harmful situations [1]; for example when a schedule is known and emotions can be mapped to a specific event.

We propose to let users decide when and to whom information is sent, to allow removals limited to periods, preventing fine tuning, and to indicate the representativeness of accessible data. Users should be incited to justify deletions. This would comfort recipients, and peer pressure may demotivate users from removing data without good reasons. For deactivation, on/off controls should be made available.

Illustration with our System. The server currently feeds on raw physiological data and copies of e-mails. An improvement would be to have a personal agent located in the wearable filter the data, process it, then transmit only intensities and emotional states to selected users, hiding raw data and preventing much additional–unwanted–inferences. The agent would inform with a precision inversely proportional to elapsed time; for a given individual "current", "day", and "month" values only being available. Data older than a month would be deleted. The "current" state can be associated by users to variable durations on a per-recipient basis. An on/off button would request the agent to finish the current transaction then stop its activities

4 User Side

The user side of the disclosure process mainly concerns its last phases: multi-modal rendering and interactions.

4.1 Multi-modal Rendering

When recipients receive data, they may be notified of the arrival of information before its rendering.

Notification. For numerous services, recipients would benefit from notifications that indicate the arrival of updates or important messages. These notifications need to be efficient enough to raise recipients' awareness about the event. Ideally, notifications themselves would provide information about received content, like what has been done with cellular phones, vibrating or ringing differently depending on whether an e-mail or phone call is received, or on callers' identity.

For systems that disclose emotional states on demand, the notification can simply inform the user that a change occurred, letting her check the information at her convenience, for example later when she is alone. For systems that disclose emotional states on a continuous basis, the notification can inform the user that a change occurred and will soon be rendered (e.g. displayed on her wearable screen), letting her modify her physical and social settings before the event. This latest type of notification implies delays in rendering, either of fixed duration based on user settings, or of variable duration based on context awareness (e.g. presence or absence of bystanders based on radio-frequency identification).

In everyday situations, there is a balance to strike between efficiency and usability. Sound notifications would be disruptive, and eventually revealing to bystanders. Vibrating notifications would be discreet but may go unnoticed during physical activities. Discreet but informative notification is a good objective however its medium and expression should be selected according to the specificities of services and users (notably from expected lifestyles).

Rendering. Information may be provided to recipients via sight, hearing, touch and smell. In all cases, the risks to privacy are related to involuntary disclosure: a bystander seeing information on the display, hearing a message, feeling vibrations, smelling unusual fragrances.

The rendering should provide qualitative rather than quantitative information. To minimize risks, access to devices should be limited: a vibrating device may be around the wrist instead of upon a table, a display can be covered with a polarized film, messages can be listened to with earphones rather than loudspeakers, etc. Beyond the designers' expectations, form-factors and affordances [5] matter.

Finally, information can be coded so as to be incomprehensible to outsiders. The code should not be easily guessed, but may be selected by the user to facilitate his memorization. With simple interfaces, coding schemes are quite limited and should therefore be changed regularly, like passwords should be. With more complex interfaces, this may not be necessary. For example, virtual environments allow so many subtle manipulations (weather conditions, presence of objects, speed of animals) that chances to accidentally understand a message are extremely low.

Illustration with our System. Our system proposes e-mail alerts, visualization in web pages or continuous updates on the screen of a wearable computer. This diversity favors universal access but increases the difficulty to efficiently preserve privacy. The e-mail alerts are expected to reach mobile devices and benefit from their usual notification schemes (e.g. vibrations, dedicated ring tones). During visualization, acquaintances are mirrored with the *soap bubbles* metaphor. In the current version, bubbles contain text indicating the acquaintance's name, and the color reflects the emotions based on a unique color scheme. We propose to let users personalize colors, shapes and sizes to represent identities and emotional states so that users do not worry about what bystanders see. Besides, bubbles should not all be visible simultaneously, to avoid inferences on the number of registered acquaintances. Wearable screens will be covered with polarized films and turned off after a few seconds of inactivity. Finally, the wearable shall be equipped with a vibration-based notification system located on the wrist.

4.2 Interactions

Services may enable recipients to react to visualized information or to emotion-related messages; risks are then related to errors of manipulation and to bystanders noticing and understanding actions carried out.

Actions. Two types of actions lead to breaches of privacy. The first one is sending a message to a wrong recipient, potentially revealing information about the intended recipient. The second comprises actions that are observed and understood by a bystander.

If a message is sent to a person in response to an event (e.g. an "anxiety" alert), the source of the alert should automatically be selected as recipient. After sending a message, the identity of the recipient should be quickly reminded to enable senders to

realize they have done an error if it is the case. Then, there should be a way to cancel sent messages as long as they have not been delivered or viewed.

Depending on the equipment, functions might be directly associated to e.g. the buttons of the physical interface. The process should include the information that is necessary to the user but in a way that is not accessible to bystanders. For example, the function of buttons should be associated to tactile labels rather than visual labels.

Feedback. The issue of feedback for interactions is related to the issue of multi-modal rendering described above. For visual feedback, if codes (colors, shapes) are used, bystanders may understand an interaction occurs but neither know what information is sent, nor to whom. Simple languages can be developed but it seems unrealistic for complex messages. It is realistic for simple messages such as "I think about you", "good luck", or "need help?"). One way to hide information to bystanders is to use touch interfaces instead of visual interfaces.

Illustration with our System. With the current design, users can send pre-defined messages, with three buttons ornamented with small drawings that indicate the nature of the message. For example a heart for "I love/support You", a question mark for "Need help?", and a OK mark for "I am fine". The selection of the recipient is done with a click on the touch screen, on the bubble associated to the intended recipient. Instead of the small drawings, we propose to put relief drawings, not visible but felt with fingers tips.

5 Global Issues

In addition to the issues cited previously, we add a few transversal issues: awareness, access, culture, and recommended practices.

Awareness. We considered so far that no additional information is provided besides emotional states. Although simultaneous communication is out of the scope we cover here, the issue of context awareness cannot be neglected. Because information is sent to acquaintances, additional information may be available to understand situations resulting in the elicitation of an emotion. At the minimum, one's schedule might be known by parents and a few friends.

Ubiquitous systems that have been foreseen may lead to the disclosure of location, co-presence, or type of ongoing activity. Appearing scared when in a vivarium can reveal a phobia of reptiles. Showing happiness or calm (boredom?) when in presence of a certain person can reveal global feelings towards that person. Being systematically walking when sad can reveal a coping practice. In such cases, how do we protect the user's privacy? Should we? *Can* we? When several services are active simultaneously, we cannot rely on them to deal with such a problem. Neither can we rely on users: they would be likely to forget to deactivate some functions or might decide that the services are too much trouble. As far as input from users is concerned,

a personal agent is required to filter the data; and for everyday uses, this agent would need to be much smarter than what artificial intelligence has provided so far.

Access. Privacy is related to accessibility, which can be digital (e.g. stored, transmitted) or physical (e.g. visible on a wrist-located display). Obstacles to access are linked to the environment, to available resources, and to the information itself; they should be exploited as often as possible when useful and practical.

Our proposal to incorporate buttons with tactile instead of visual labels exploited the obstacle of distance. Similarly, providing useless information would add the obstacle of noise. Digital information is much more sensitive in the sense that it is permanent and that memory and processing capabilities are not real problems anymore; only the time to carry out operations remains a tangible obstacle.

Finally, privacy can be threatened if a personal device containing information becomes accessible to an outsider, even if only for a few seconds. This problem can be solved by requesting strong but convenient identification, and by deactivating the device when its owner is not around. Identification can be based on biometrics (e.g. fingerprints), and deactivation can be enforced with the use of an external token [6].

Cultures. When considering the creation of universal services, attention must be paid to cultural factors. People from different countries may share a minimal conception of privacy but not rich ones, leading to clashes when worldwide services emerge [7]. Privacy requirements will–and implementations should–vary:

> "One insight that clearly arises in examining privacy in Japan and elsewhere is the important role trust plays in support of privacy and how the mechanisms of trust can be manifested differently in different cultures.", Mizutani et al. [7]

Bell [8] highlights cultural specificities for actual ubiquitous services, notably in Singapore, at the opposite of the Western-oriented research. Of course the problem is not limited to groups of users but extends to interactions between users of different cultures. Such a situation hints at the interest of contracts sent alongside emotional information, stating how the received information may be used.

Recommended Practices. The ACM's code of ethics [9] provides principles concerning the respect of privacy in section 1.7: *Respect the privacy of others*. These principles were included and adapted in our discussion. Marx also guides system designers with 30 questions that determine the ethics of surveillance [10]. None of these guides however concern emotional data per se.

6 Future works

In this paper, we discussed privacy issues for the disclosure of emotions in one specific but significant case. Our goal was to clarify basic privacy issues before implementing a related system. Our next steps will accordingly be to create the system, evaluate

the pertinence of our proposals, and identify additional issues. We will be interested in checking users' perception of the privacy solutions, and evaluating the influence of these solutions on the acceptance and usability of the system. Finally, we need to investigate in more depth several aspects' of our visual interface: how would colors and shapes be associated to family members and friends? Do patterns emerge, reducing the usefulness of the scheme for privacy? Answers could be exploited in both affective computing and security/privacy communities.

References

1. Duval, S., Hashizume, H., Andrès, F.: First Evaluation of Enhanced Jackets' Potential to Support First Encounters with Photo Slideshows and Emotional Displays. 8th Virtual Reality International Conference. (2006) 75-84
2. Ekman, P., Davidson, R.: The Nature of Emotions – Fundamental Questions. (1994)
3. Gotterbarn, D.: Privacy lost: The Net, Autonomous Agents, and 'Virtual Information'. Ethics and Information Technology. (1999) 1:2, pp147-154
4. Duval, S., Hashizume, H.: First Design of a Ubiquitous System for Affective Bonding and Support with Family and Friends. 2nd International Conference on Online Communities and Social Computing, HCII. (2007) in press
5. Gibson, J.: The Ecological Approach to Visual Perception. (1979)
6. Nicholson, A., Corner, M., Noble, B.: Mobile Device Security Using Transient Authentication. Transactions on Mobile Computing. (2006) 5:11, pp1489-1502
7. Mizutani, M., Dorsey, J., Moor, J.: The Internet and Japanese Conception of Privacy. Ethics and Information Technology. (2004) 6:2, pp121-128
8. Bell, G., Dourish, P.: Yesterday's Tomorrows: Notes on Ubiquitous Computing's Dominant Vision. Personal and Ubiquitous Computing. (2007) 11:2, pp133-143
9. ACM Code of Ethics. <http://www.acm.org/constitution/code.html> (checked on 2007, February 16th)
10. Marx, G.: Murky Conceptual Waters: the Public and the Private. Ethics and Information Technology. (2001) 3:3, pp157-169