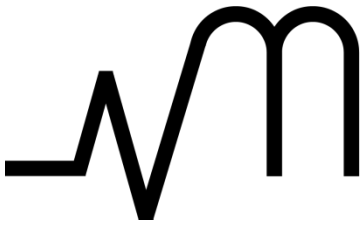

MindSee: Symbiotic Mind Computer Interaction for Information Seeking

FP7-ICT-2013-10 (STREP)

GA: 611570

Deliverable 1.3

Report on ethics, acceptance, and design of symbiotic system

Authors Luciano Gamberini (UNIPD), Anna Spagnolli (UNIPD), Patrik Pluchino (UNIPD), Simone Zanoni (UNIPD), Giuseppe Sartori (UNIPD), Sara Mondini (UNIPD), Valeria Orso (UNIPD), Marta Nedves (UNIPD), Paolo Negri (UNIPD), Francesco Chiossi (UNIPD)

Version v1.0

Date 31.09.2016 (postponed to 31.10.2016)

Classification Public

Contract Start Date 01.10.2013

Duration 36 months

Project Co-ordinator University of Helsinki

File Name MindSee D1.3 f1.0 UNIPD

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 611570

Consisting of:

No	PARTICIPANT NAME	S.N.	COUNTRY
1	University of Padova	UNIPD	IT
2	Golsmiths	GOLD	UK

Responsible of the document: UNIPD

Defined Contributors to the document: Luciano Gamberini (UNIPD), Anna Spagnolli (UNIPD), Patrik Pluchino (UNIPD), Simone Zanoni (UNIPD), Valeria Orso (UNIPD), Marta Nedves (UNIPD), Paolo Negri (UNIPD), Francesco Chiossi (UNIPD).
For Annex IV: Aimee van Wynsberghe (MindsEE advisor, University of Twente, the Netherlands), David Kirsh (MindSee advisor, University of California, San Diego, US), Jonathan Freeman (GOLD), Mauro Conti (UNIPD), Giorgia Guerra (UNIPD).

Other Expected Contributors: -

Executive Summary

PROJECT SUMMARY

The MindSee (Symbiotic Mind Computer Interaction for Information Seeking) project's main objective is to exemplify the fruitful symbiosis of modern BCI technology with a recent real-world HCI application to obtain a cutting-edge information retrieval system that outperforms state-of-the art tools by more than doubling the performance of information seeking in realistic tasks.

More specifically MindSee will develop techniques to co-adapt user and computing systems utilizing implicit information such as EEG phenomena coupled with peripheral physiology during search to detect comprehensive user responses ranging from preconscious perception, cognition and emotion. Such implicit information feeds into a user model in reinforcement learning allowing to co-adapt exploration and exploitation in information seeking in relevance of information, complexity and aesthetic aspects. MindSee will capitalize on recent advances in BCI combined with peripheral physiological signals (EDR, facial EMG, eye gaze and pupillometry) for an unobtrusive registration of user states at a highly resolved level with respect to perception, cognition and emotions. Combined with machine learning based co-adaptation approaches this will allow predicting user intention for an unprecedented man-machine symbiosis.

DELIVERABLE SUMMARY

This document contains the results of WP1 activity in Y3. The activity addressed receipt, acceptance and risks of symbiotic systems. Three studies were carried out to this purpose and an interdisciplinary panel of experts was gathered to shed light on these issues. The first study showed that the users' response to an implicit input modality can be of unease even though performance is higher than with a traditional, mouse-based modality. We hypothesized that lack of feedback and transparency might be the reason. The second study found that users rate the system higher in quality and credibility when it is fed with sensitive data and when such data is collected explicitly. Our explanation is that they rely on an effort heuristic to retrospectively justify the risky choice of explicitly releasing sensitive data. The third study found that providing explanations of the implicit collection of sensitive data increases the credibility of the system and its perceived quality; it also reduced the frequency of further risky behaviour (i.e., waving anonymity).

All studies point at the value of transparency in symbiotic systems but remind that transparency effects increases with the comprehensibility of the explanation provided and can have the counter-effect of triggering defensive mechanisms in the user. The international ethic panel of experts we inquired gave insightful cues as to the way to frame and then minimize the risks for users; in particular it was suggested how distributing the job of protecting the user might be preferable to a mis-interpreted emphasis on transparency that charges only the user with all the burden of dealing with the risks of releasing personal information. It also emphasized the importance of increasing awareness of the value of sensitive data at a societal level.

Table of Contents

List of figures

List of tables

1 Progress for the Year

1.1 Studies

1.1.1 Study 1: Users' response to implicit vs. explicit input modalities

This first study evaluates how implicit (e. g, gaze-operated interface) vs. explicit (mouse) input modalities are received by the users. Although all commands are given deliberately by the user in this study, the gaze-operated interface was considered as adopting an implicit input modality because the same body part was used to receive the computer output and to provide input, in a switch between receiving and sending behavior that only the system could detect with precision. Participants used both input modalities to accomplish the same tasks on the MindSee interface. Both objective and subjective measures (i.e. usability, pleasantness, utility, and accuracy of the system) were collected.

Findings showed that participants in general were faster in accomplishing a task when they interacted with the system utilizing their gaze compared to when they utilized the mouse, even though the latter were more familiar. Considering the emotions experienced and the level of activation the only significant difference regarded the maximal level of emotional valence, which was higher when the participants were interacting with the system by means of the eye gaze controls compared to the traditional mouse controls. This might be interpreted as a sign of unease. Indeed, the subjective evaluations of accuracy, easiness, and efficiency were lower when using the gaze-operated interface; gaze-operated controls out-performed the mouse only in terms of pleasantness.

The lower subjective evaluation of the accuracy and efficiency of the eye gaze - vis-s-vis their higher performance - could be due to the lack of feedback regarding the actual coordinates of the command sent to the interface (e.g., position and length of the users' gaze target on the screen), and could be improved by making such coordinates transparent to the user.

1.1.2 Study 2: Explicit vs implicit acquisition of sensitive data and effect on credibility

The study considers that the implicit acquisition of personal and potentially sensitive information is one of the characteristics of symbiotic systems that can be most dangerous to users. It also stems on the assumption that the consent to use such data is given quite superficially, instrumentally to receiving a service of interest; so most users are to face the consequences of such decision more than they dwell on the decision itself. This study then investigates the psychological processes *following* data disclosure. The rationale of the study hypothesizes that an effort heuristic is at work, such that if the user considers that s/he has made a risky decision, namely one that can have some serious costs to him/her, then s/he tends to justify such decision by overestimating the value of the service received as a consequence of that decision. This type of heuristic is known both in social psychology and in the psychology of decision making and is expressed in many forms: self-justification in the decisional process (Staw, 1981), effect of a heavy initiation on group evaluation (Aronson Mills 1959); effort heuristic (Kruger et al, 2004). We then hypothesized that the user would better evaluate the system that s/he has explicitly fed with sensitive information.

The system used in the study is a social network of academic scholars and the task consists of finding the connections of one the participants' professors. The sensitive data allegedly acquired by the system was the positive or negative opinion about such professors, acquired either via questionnaire (explicit modality) or via visual behaviour while looking at the image

of the professor on the social network (implicit modality). 36 students volunteered to participate in the study. The results confirm the hypotheses, showing that users rated the system quality (accuracy, credibility, usability) higher in the explicit data acquisition condition than in both the implicit data acquisition condition and in the control condition where no sensitive data was acquired.

The study suggests that users tend to justify the release of sensitive data by retrospectively overestimating the quality of the service to which they have given the data. In other words they might try to act defensively by justifying their risky behaviour as worthwhile.

1.1.3 Study 3: Effect of implicit systems explainability on credibility

This third study in the document tests the effect of explainability on the credibility of a system collecting data in implicit modality. In other words it tests whether making the acquisition of implicit data more transparent to the user would increase the credibility of that system, as is suggested by the literature showing that explainability can increase the user experience of a system (Tintarev, Masthoff, 2007). Based on the results of the second study it also aims to test the effect of transparency on the overall evaluation of the system, as an effect of the effort heuristic; in other words, it tests whether making an implicit system more transparent would make clearer to the user the riskiness of the information s/he is releasing and then set the basis for a defensiveness effort heuristic when asked to evaluate the quality of the system s/he had fed with personal data.

The sample is constituted of 36 participants with a task similar to the task used in the second study, namely to enter a query in a social network for academic researchers returning the connection between researchers based on co-authored papers. The user was connected to the eye-tracker to allegedly collect their responses to the images of their professor appearing in the social network graph. The extent to which the nature of the data allegedly collected was explained to the user was varied (no explanation, explanation about the type of data, explanation about the meaning of the data). The result confirmed the hypothesis: as the explainability increased both credibility and quality of the system were rated higher.

This study suggests that increasing the transparency of the data collected implicitly improves the credibility of the system in the eye of the user; at the same time, it makes the user more defensive, leading the user to magnify the quality of the system s/he has fed with sensitive data.

1.1.4 Framing and minimizing ethical, legal and security risks for users: results from SYMBIOTIC 2016 interdisciplinary panel

In order to reflect about the way in which everyday life applications of symbiotic systems can bear some problematic implications for the users, a panel of experts was organized to cover the possible risks from different points of view: ethics (Aimee van Wynsberghe, President of the Foundation for Responsible Robotics and Assistant Professor at the University of Twente, the Netherlands), information security (Mauro Conti, University of Padua, Italy); law (Giorgia Guerra, University of Padua, Italy), human-computer interaction (David Kirsh, University of California, San Diego, US) and psychology (Jonathan Freeman, University of London, Goldsmith College, UK perspective).

The panel met in Padua on September 29th. The discussion focussed on three main characteristics of symbiotic technologies that might be problematic when the aim is to protect users from undesirable consequences:

- *acquisition of implicit data*, namely data that users might not be aware of giving out and whose release and content they might not be able to control;

- a *model of the user* is created out of the data collected;
- *decisions* are made on the users' behalf, according to the user's model and to what it is programmed to consider as the best way to serve that model of the user.

These characteristics were identified based on Y1 and Y2 activity in defining core aspects of symbiotic systems (e.g., Jacucci et al, 2014), on the MindSee D1.4 where some of these risks were preliminarily listed and on the outcome of other projects (e.g. Langheinrich, 2013)

To help discussion, three cases were created where symbiotic technology application to everyday life could generate some risks for the users' privacy, identity or security.

Each panellist was provided with the cases in advance and was invited to reflect on the way to frame the risks to users evoked by each case in terms of his/her own expertise, as well as to identify possible solutions to minimize such decisions. The full edited transcript of the panel is reported in Annex IV and will be included in the Springer proceedings of Symbiotic 2016.

Overall, panellists were able to provide very clear solutions to understand the nature of the risks and to face them. A recurrent theme was the need for *relieving* the user from being the only one charged with his/her own protection, as well as the need to increase *awareness* of the risks of current systems and enforcing pervasive solutions at various levels in society.

1.2 Achieved objectives

Here are described the objectives of Work Package 1 is titled "Symbiotic scenarios and user experience" according to MindSee Description of Work document, and the extent to which they are achieved.

a) describing the scenario of MindSee system usage

This objective was 100% achieved in Y2.

b) identifying the user requirements of MindSee interface and design core functionalities

This objective was 100% achieved in Y2.

c) outlining the relevant dimension and related metrics to measure user experience (including the accomplishment of some usability test on early prototypes, Ms2)

This objective was 100% achieved in Y2.

d) defining the core notions of symbiotic systems;

This objective was pursued continually throughout the project's life. In Y3, it was pursued via the 5th Symbiotic workshop organized by the beneficiary responsible for WP1, i.e., UNIPD. The workshop proceedings will be published by Springer.

e) exploring the possible societal and ethical implications of symbiotic systems as well as the factor affecting their credibility and acceptance.

Three studies were carried out in Y3 to investigate users' response to a symbiotic system as such; the studies (N = 59, 36, 36) compared implicit vs. explicit input modalities and measured users' evaluation of the system quality, credibility and users' emotional responses (section 1.1.1, 1.1.2, 1.1.3 and Annex I, II, III).

In addition, a panel on the ethical, legal and security risks to users possibly derived from unwise applications of Symbiotic Systems was included in the Symbiotic 2016 workshop; it involved two project's advisors (A. van Wynsberghe and David Kirsh), and experts Giorgia Guerra and Mauro Conti in addition to consortium members Anna Spagnolli (UNIPD) and

Jonathan Freeman (GOLD). The panel allowed to frame those risks and to consider some minimizing measures from an interdisciplinary perspective (law, security, design, ethics) (section 1.1.4 and Annex IV).

The objective was then 100% achieved.

1.3 Answer to Monitors' Comments

During the second review, monitors formulated the following remarks about WP1 activity. Below is described how these remarks were taken into account.

REMARK: "Study could benefit from a comparison of results of usability questionnaires with another (baseline) system. Take care of the balance of practice/use vs evaluation time for subjects (effect size can increase with longer use)."

ANSWER: In the studies belonging to T1.4 and reported in this deliverable we have systematically compared symbiotic characteristics with non-symbiotic ones. In the studies all users were mostly not familiar with the system (the MindSee interface or a social network for academics). In addition. a training session preceded all experimental sessions, and the prior familiarity of the user with the systems was measured.

REMARK: "Can facial emotion detection be better integrated, as measurement between conditions/systems or be left out? Now it is hard to interpret the measured values."

ANSWER: Study 1 in this deliverable uses facial emotion detection and integrates emotion measures as one of the dependent variables to compare the different conditions.

2 Annex I: Study 1

The study is intended to evaluate how the eye tracking features implemented in a prototype of the MindSee interface are received by the user compared with a traditional, explicit input modality (i.e., mouse). With this aim, eye gaze commands were implemented in MindSee interface and used vis-a vis the mouse to carry out three tasks (opening an abstract, bookmarking an abstract and highlighting the abstract's keywords); users' performance and evaluation of the two types of controls were then compared.

2.1 Method

2.1.1 Participants

Fifty-nine students from the University of Padua were involved in the experiment on a voluntary basis. Eight participants were eventually excluded as outliers in terms of temporal session duration or for bad quality of the videos recording and the impossibility to analyze them with the Face Reader. Data from 51 students (F = 23) with a mean age of 27.05 years (sd = 3.87) were then analyzed. All participants had normal or corrected-to-normal vision and gave their informed consent.

2.1.2 Apparatus

The experiment was conducted in a small closed room enlightened by a neon bulb. No external lighting sources were allowed, in order to maintain a constant level of illumination in the room. The adopted equipment consisted of several devices. A remote eye tracker, namely an SMI RED 500 (SMI™), with a sampling frequency of 500Hz was utilized to record eye-related data and pupil diameter.

A laptop DELL LATITUDE E6530 Notebook, implemented with Windows 7 Operative System 32-bit, Intel core i7-3540M CPU @ 3GHz and 4.00 GB RAM, was utilized to store the eye tracking data and to evaluate the calibration quality through iViewX software version 2.8 (SMI™).

A desktop computer, implemented with Windows 7 Operative System 64-bit, Intel Xeon CPU E5-2620 @ 2.10 GHz (2 processors) and 16.00 GB RAM was utilized for performing the eye tracker calibration through the Experiment Center software version 3.6 (SMI™).

A desktop computer MacPro, implemented with El Capitan Operative System 64-bit, a 3.7 GHz Quad-core Intel Xeon E5 and 32.00 GB RAM hosted the MindSee application. This computer was connected to a 22'' DELL monitor with a resolution of 1680 x 1050.

Moreover, the participants were video-recorded, utilizing a QuickCam Pro 9000 (Logitech®) that presents a maximal resolution of 1600 x 1200, during respectively the baseline and the experimental session. Moreover, a two halogen bulb lights (60W) were placed at both ends of the screen in order to improve the quality of the video-recordings.

A DELL XPS 27" Desktop, mounting Windows 8.1 64-bit, Intel core i7-4770S CPU @ 3.10 GHz and 16.0 GB RAM) hosted the FaceReader6 application that was employed to analyze the videos acquired using the previously mentioned webcam. The FaceReader allowed evaluating participants' proportion of different emotions and arousal levels experienced during the two interactions with the MindSee interface.

In order to connect all the devices a TL-SF1005D Ethernet switch was utilized.

2.1.3 Stimuli

The MindSee interface was presented utilizing an application that was developed in c++. In each screen the interface presented a query field, an orbitarium in which several keywords are presented (polar coordinates are considered in order to arrange the keywords). A set of papers is presented to the right side of the orbitarium. This list contains the documents that were retrieved by the system after a search iteration. The interface allowed to enter new queries, give relevance feedback to the keywords (by drawing them closer or further away from the center of the orbitarium and pressing a "refresh" button) and to read the abstracts of the articles returned after the query and listed on the right of the screen.

According to the task, the MindSee application allowed to perform those actions with the eye gaze. In particular, it allowed:

- *abstract opening*, i.e., users could open an abstract by simply looking at it for at least three seconds (non-cumulative) (Figure 1);

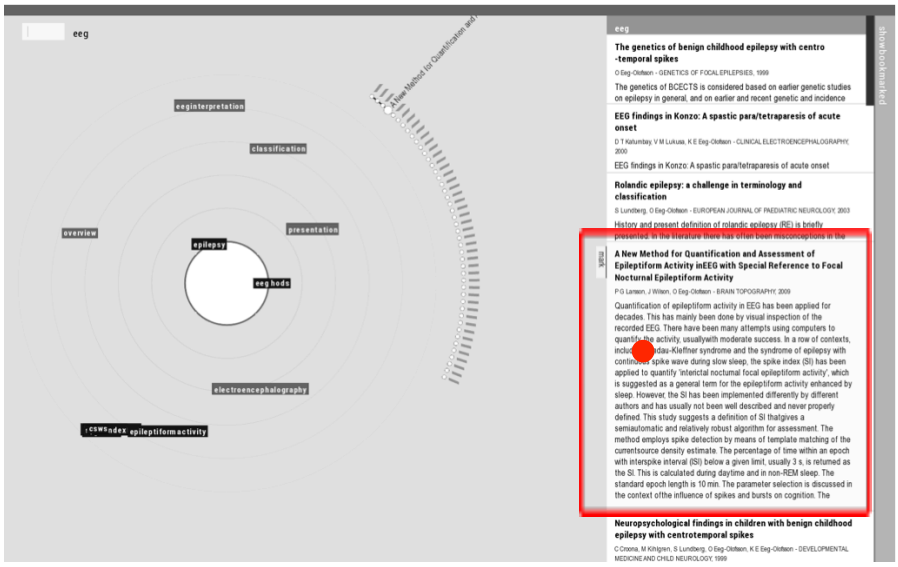

Figure 1 Abstract opening utilizing the gaze (the red dot corresponds to the gaze position).

- *gaze bookmarking*, i.e., users could bookmark an abstract by just looking at it for at least five seconds (in a non-cumulative way (Figure 2);

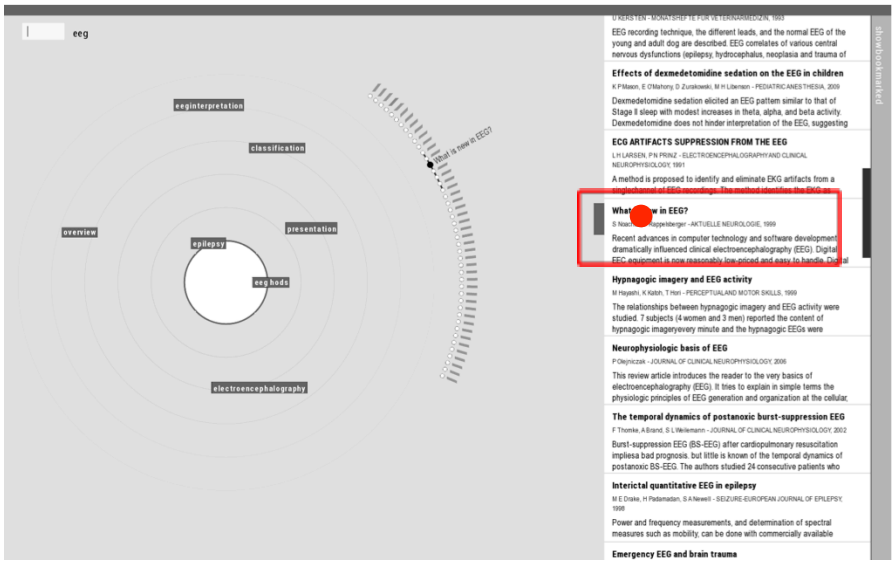

Figure 2. Abstract booking utilizing the gaze (the red dot corresponds to the gaze position).

- access to all the keywords that were linked to each of 7 chosen abstracts at will using their gaze (when the eye-tracking feature was the keywords fade in and out, Figure 3).

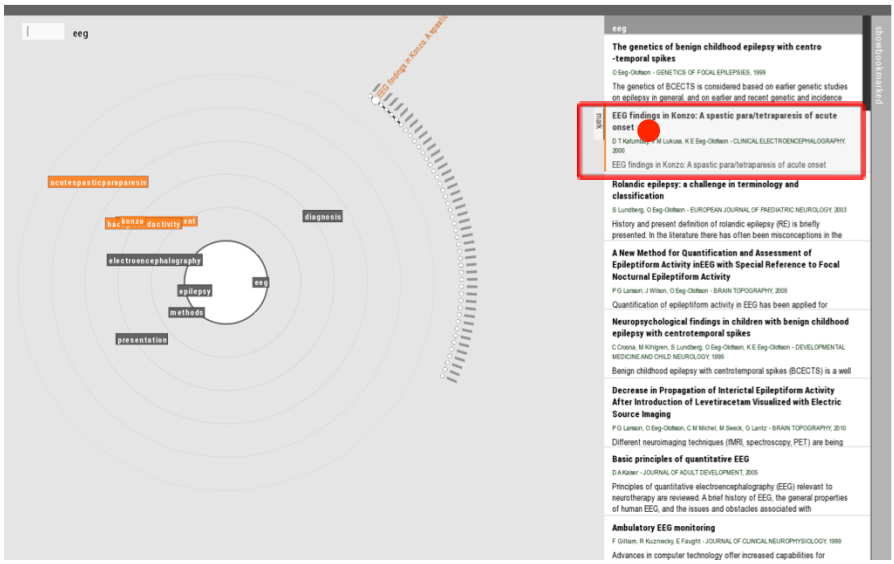

Figure 3. Keywords fade in and out utilizing the gaze (the red dot corresponds to the gaze position).

2.1.4 Design

Two factors were independently manipulated within the current experiment (mixed-design). The within-participants factor was the type of controls (eye gaze vs. mouse) utilized to accomplish the tasks. The between-participants factor was the kind of task that participants had to perform (*abstract opening* Vs. *gaze bookmarking* Vs. *keywords fade in and out*). (17 participants in each condition)

2.1.5 Procedure

Upon arrival, participants were welcome and they were asked to read a document that

contained general information about the study. Moreover, an informed consent was administered. Participants were seated at approximately 60-70 cm away from the screen. They were asked to find a comfortable position and to avoid head and body movements for the whole duration of the test. In the mouse controls phase the participants inputted commands in the system using the mouse; the topic in this session was "database". At the beginning of each eye gaze controls phase (the topic in this session was "machine learning") the eye tracker was calibrated (i.e. the distance between the sight position and the tracked position was maintained below 0.5 visual angle degree). The procedure was a 5-point calibration. The phase order (i.e. mouse and eye-tracking) was counter-balanced across participants. Before each phase, participants underwent a training session to familiarize with the interface and its controls; "EEG" and "ERPs" were used as topics for the query.

At the end of both phases, participants were administered an electronic questionnaire evaluating the system. Upon completion of the questionnaire, they were debriefed about the purpose of the study and the experimenter answered questions. The experiment lasted about 20-25 minutes.

2.1.6 Measures

Objective and subjective measures were taken during and after the session:

- *Temporal session duration*. The total time (in sec) needed to accomplish the task
- *Percentage of experienced emotions*. The *percentage of experienced emotions* (positive and negative ones) during the experimental sessions.
- *Maximal level of emotional valence.* The maximal level of emotional valence (that can vary between -1 and 1) during the experimental sessions.
- *Maximal arousal level.* The level of general activation of participants (that can vary between 0 and 1) during the experimental sessions.
- *System evaluation.* An ad hoc user experience questionnaire (10 items for each type of controls; total of 20 items) was administered to collect the users' evaluation of the following aspects on a 5-point scale (1 = not at all; 5 = very): usability (easiness, efficiency, fatigue, clarity, speed, fluidity, intuitiveness), pleasantness, perceived utility and accuracy of the system.

2.1.7 Data analyses and pre-processing

Some of the following analyses were conducted by means of mixed-models (generalized in accordance with data distribution). The fixed effects were the experimental task (*abstract opening* Vs. *gaze bookmarking* Vs. *keywords fade in and out*) and the controls (mouse Vs. eye gaze) utilized to perform the different tasks. Participant was included as random effect. In all these analyses the abstract opening task and the mouse controls were set as the contrast levels.

FaceReader data were pre-processed using a series of customized functions realized in MATLAB (Release 2015a, Mathworks Inc.).

At a second stage, the statistical analyses were performed utilizing the R Version 0.99.903 and the R package lme4 (R Core Team, 2015) and in order to deal with percentage (i.e. emotions analyses) two beta regression analyses were performed utilizing the betareg package (Cribari-Neto & Achim Zeileis, 2010).

The experimental sessions that were considered outliers in terms of the temporal duration were excluded employing the interquartile range procedure (i.e. all values falling outside 1.5 IQR from the extremes of the IQR box were considered outliers). This procedure was applied to each singular experimental task (i.e. *abstract opening*, *gaze bookmarking*, and *keywords fade in and out*).

2.2 Results

Temporal session duration (generalized mixed-models)

On the mean temporal duration of task completion a main effect of the task was found. Participants were faster in performing the task when they have to bookmark the papers (b = -0.82, t = -4.05, $p < .001$; M = 165.76 sec) and when they have to access to all the keywords of each abstract (b = -0.49, t = -2.41, $p < .05$; M = 244.67 sec) compare to when they have to open the abstracts (M = 373.07 sec; see Figure 4).

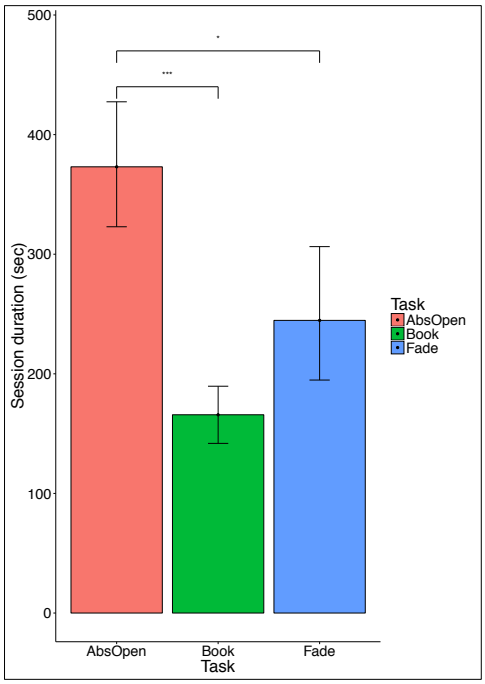

Figure 4. Mean duration of an experimental session as a function of task.

Furthermore, a main effect of the controls emerged (b = -0.15, t = -2.15, $p < .05$). Participants were in general faster in accomplishing the tasks when they utilize eye gaze (M = 247.34 sec) compared to mouse (M = 274.99 sec; see Figure 5). No interaction between fixed effects emerged.

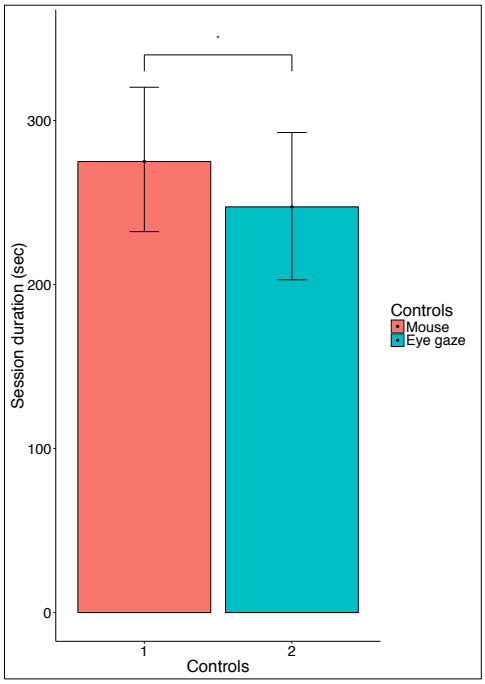

Figure 5. Mean duration of an experimental session as a function of controls.

Percentage of positive emotions (beta regression)

No main effect on the percentage of positive emotions was found. Participants experienced similar percentage of positive emotions despite the controls and the task (see Table 1).

Table 1. Percentage of positive emotions experienced as a function of controls and task.

	Controls	
	Mouse	Eye gaze
Tasks	*M*(sd)	*M*(sd)
Abs Opening	13.59(17.40)	14.40(18.33)
Bookmarking	9.52(10.93)	12.38(15.78)
Fade In/Out	17.61(18.63)	14.68(17.32)

Percentage of negative emotions (beta regression)

No main effects on the percentage of negative emotions emerged. Participants experienced similar percentage of negative emotions despite the controls and the task (see Table 2).

Table 2. Percentage of negative emotions experienced as a function of controls and experimental task.

	Controls	
	Mouse	Eye gaze
Task	*M*(sd)	*M*(sd)
Abs Opening	42.64(24.09)	37.95(22.16)
Bookmarking	53.54 (32.93)	47.12(34.81)
Fade In/Out	30.70(24.56)	36.43(29.05)

Maximal level of emotional valence (generalized mixed-models)

A main effect of the controls on the maximal level of emotional valence in each experimental session was found (b = 0.07, t = 2.80, $p < .05$); see Figure 6). The maximal level of emotional valence was higher when utilizing the eye gaze controls (M = 0.83) compared to the mouse (M = 0.73)

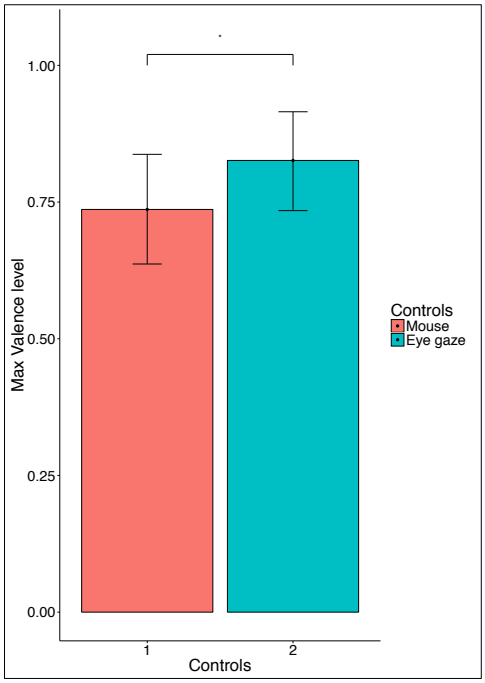

Figure 6. Maximal emotional valence level as a function of controls.

Maximal arousal level (generalized mixed-models)

No effect was found on the arousal peak in each experimental session (see Table 3).

Table 3. Maximal arousal level as a function of controls and experimental task.

	Controls	
	Mouse	Eye gaze
Task	*M*(sd)	*M*(sd)
Abs Opening	0.66(0.13)	0.60(0.13)
Bookmarking	0.59(0.13)	0.56(0.16)
Fade In/Out	0.59(0.12)	0.58(0.13)

In general the maximal level of arousal experienced by participant was similar despite of the controls utilized or the specific tasks that they have to perform.

Users' self-reported evaluation

A series of Wilcoxon rank sum tests was carried out on each questionnaire item in order to evaluate potential differences due to the manipulation of within-participants factor (*controls*). Some items showed differences in their mean scores (Figure 7): accurate (W = 1743, $p < .01$), efficient (W = 1697, $p < .05$), easy (W = 1626.5, $p < .05$), pleasant (W = 725, $p < .001$), and tiresome (W = 868.5, $p < .001$). P-values were adjusted for multiple comparisons utilizing the BH method (Benjamini & Hochberg, 1995). Participants perceived the system as more accurate, easy, efficient, and as less tiresome when they utilized the mouse. Instead, they perceived the system as more pleasant when they interacted with it by means of their eye gaze. No differences emerged in the other items (Figure 8).

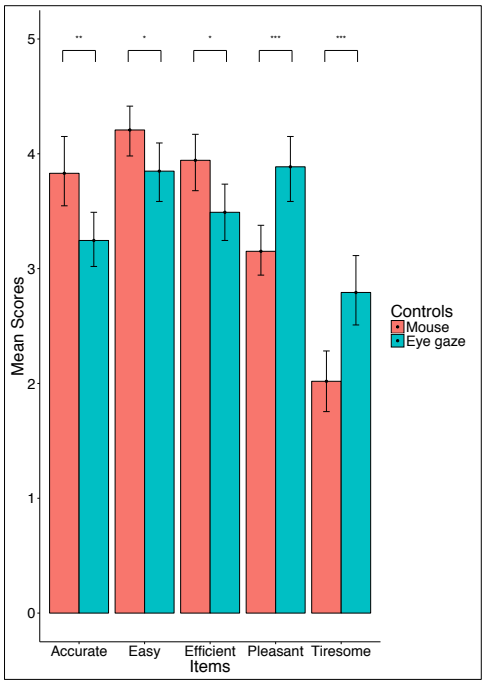

Figure 7. Mean scores for items that showed differences as a function of controls.

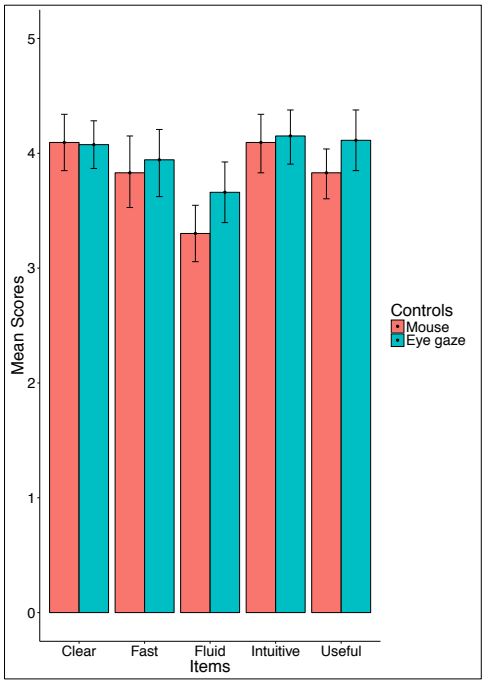

Figure 8. Mean scores for items that did not show differences as a function of controls.

Finally, delta values were computed for each pair of scores pertaining to the same item (e.g. easiness item: mouse controls score – eye gaze controls score). A series of Kruskal-Wallis rank sum tests was performed on these delta values in order to assess potential differences in the scores due to the between-participants factor (*eye-tracking feature implemented*). No differences emerged as a function of task. These tests were performed in order to evaluate potentials interactions.

2.3 General Discussion

The results showed that in general the participants were faster in accomplish the tasks when the means for interaction was the gaze. In terms of emotional response, the maximal arousal level and the percentages of experienced emotions suggest that the stimuli per se had low emotional valence; nonetheless, participants' response showed a higher level of emotional valence while utilizing the eye gaze control. [1] This, along with the lower subjective evaluations of accuracy, easiness, efficiency and fatigue reveal a higher cost of the eye gaze both practical and emotional despite the superior performance. This cost is due in part to the position they had to maintain in order to allow full functionality of the eye-tracker (head must be still) and in part to the lack of transparency about the system's processing of the eyegaze controls.

[1] The general higher percentages of negative emotions experienced (35-53%) could be accounted for the reason that some of the muscles involved in the negative emotions (e.g. corrugator supercilii, procerus, frontalis) are also involved in situations of high focus in performing a task and that in accordance to the literature (Stekelenburg & Boxtel, 2002) it could be considered as "an expression of voluntary attention elicited by the stimulus".

3 Annex II: Study 2

In this study the user is asked to release sensitive data either explicitly or implicitly to feed a system, and is asked to evaluate the system after using it. In a third condition the user gives non-sensitive data. In this way the study aims to check whether there is an effort heuristic (Kruger et al, 2004) at work, which would increase the system evaluation in the condition where sensitive data are released explicitly.

3.1 Method

3.1.1 Design and hypotheses

One between-participants variable, data sensitivity, at three levels (no sensitivity, explicit sensitive, implicit sensitive). Sensitive data in this study are the participants' positive or negative opinion about his/her professors.

- *No sensitivity* (control condition); the participant is asked for demographic data (date of birth, gender, mother tongue), familiarity with the social network for academics used in the study and attitude towards innovation and privacy.

- *Explicitly sensitivity*: in addition to the data collected also in the control condition, in this condition the participant is asked, before using the social network interface to search his/her professor's connections, to explicitly evaluate those professors' sympathy, attractiveness, availability on an anonymous questionnaire as well as the extent to which it evoked sadness.

- *Implicitly sensitivity*: in addition to the demographic and familiarity data, the participant is asked to use an eye-tracker when examining the social network graphs of his/her professors to allegedly collect the participant's positive or negative reaction to the image of the professors displayed in the social network graph.

The hypotheses are the following:

H1: System evaluation in the explicit condition is higher than in the control condition.

H2: System evaluation in the explicit condition is higher than in the implicit condition.

3.1.2 Apparatus

- Eye-Tracking Tobii 1700 (17" & 50 herz)
- Toshiba Satellite P70-B-10T (Windows '98) to manage the calibration software of the eyetracker and administer the forms
- Webservice "Academia Search Visualizer" of Microsoft Academic (Figure 9).

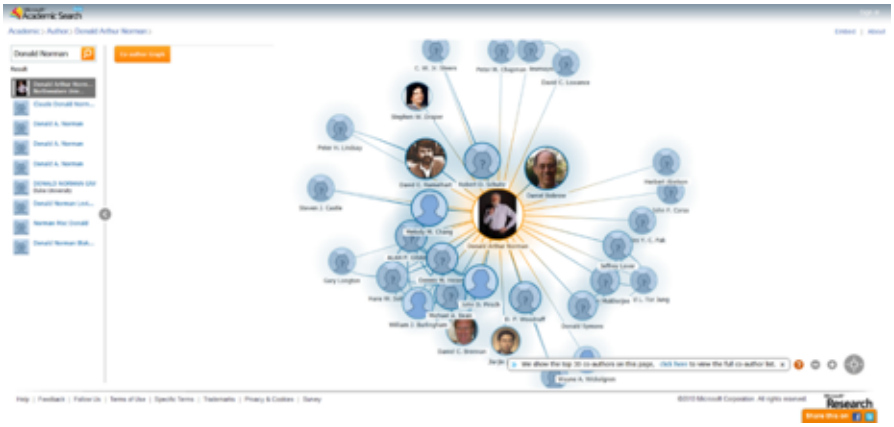

Figure 9. One screenshot from the academic social network site used in the study, in particular the page with the social network graph.

3.1.3 Measures

Pre-session questionnaire

- *Demographic data*, collected via a short questionnaire before the session;
- *Familiarity* with the social network system used in the study, collected via a short questionnaire before the session and measures in a 4-degree scale (none, poor, moderate, advanced);
- *Personal Innovativeness* (Lu, Yao et al. 2005), subscales 1,2,3,4, where answers are collected on a Likert scale ranging from 1 (totally disagree) to 6

Post-session questionnaire included in this order:

- *System evaluation:* An ad hoc questionnaire composed by 19 statements about the systems' quality (Items 1 to 9 measuring the extent to which the system was readable, comprehensible, clear, graphically good, quick innovative, useful) and credibility (10 to 19 measuring the extent to which the system output was considered accurate, credible, informative, interesting, relevant, updated, objective, and the system producers were authoritative, expert), whose answers were collected on a Likert scale ranging from 1 (totally disagree) to 5.
- *Level of perceived sensitivity* of the data given, checked by three post-session items (do you think that the data collected was sensitive namely they were able to identify you counterproductively? Do you think that the data collected might be embarrassing to you? Do you fear that the data collected might be offensive to the professors?); answers were collected on a 5-degree scale were 1 meant not at all.
- *Concern for Information Privacy* (Korzaan, Brooks and Greer, 2009), where answers are collected on a Likert scale ranging from 1 (totally disagree) to 7

Scores of items that were formulated negatively were inverted before the analysis so that high values always mean a good perceived quality of the system.

All questionnaires were administered in electronic form.

3.1.4 Procedure

The participant is invited to participate in a study that aimed at collecting popularity rates of a social network in order to improve the kind of information on which the network currently is based. The goal was then to create a social network based on the popularity rates collected in the study. The study then involves a certain level of deceit and adopted several measures to protect the participant, including debriefing and a second consent to data usage after debriefing. It obtained the approval of the local ethical committee, at the University of Padua.

When the participant started the session s/he was first asked to give written consent to participate in the study. The participant was then randomly assigned to one of the conditions, and was asked to fill in the pre-session questionnaire. In the implicit condition the participant was also shown the eye-tracker component of the computer and instructed that the data on eye-gaze would be subsequently used to infer the users' response to the images of the professors in the social network graph. Then the eye-tracker was calibrated.

A printed tutorial explaining the Visualizer commands of relevance to the study was then offered to the participant. Subsequently the participant performed the tasks. They entered the query in the Visualizer, consisting of the name of a professor; then they had to visualize the co-author graph and write down the most common co-author of that professor. (Professors belonged to the course in which students were enrolled and were ascertained to be present with a picture in the visualizer) The task was repeated four times, 2 times by entering the name of a male professor, and 2 times the name of a female professor. Before each task, in the explicit condition the questionnaire was administered to evaluate the professor; its data were not used as a measure in the study but only as a means to manipulate the 'sensitivity' variable in this condition.

Once the fourth query task was completed, the participant was asked to fill in the post-session questionnaire.

After the completion of the data collection of the study, participants were re-contacted, debriefed and asked for their consent to use the data.

3.1.5 Participants

The sample is constituted of 36 participants (aged 23.53 years on average, SD = 1.612), 18 women, 18 men. All participants are students or trainees at the School of Psychology, University of Padua. All participants have been assigned to one condition randomly. Only one participant declared to be moderately familiar with the social network used in the study.

3.2 Results

The scores of system quality and credibility are displayed in Figure 10. The effect of information sensitivity on system quality and credibility was tested with a multivariate ANOVA, finding a significant effect, $F(4, 64) = 12.64$, $p < .001$, $\eta 2p = .44$. The univariate analysis showed a difference in both scores, system quality $F(2, 33) = 13.469$, $MSE = 16{,}123$ $p < .05$, $\eta 2p = .632$ and system credibility, $F(2, 33) = 13.755$, $MSE = 13{,}545$, $p < .05$, $\eta 2p = .67$. The pairwise comparisons with Bonferroni correction showed that the explicit condition has higher scores than the control and the implicit condition ($p<0.5$).

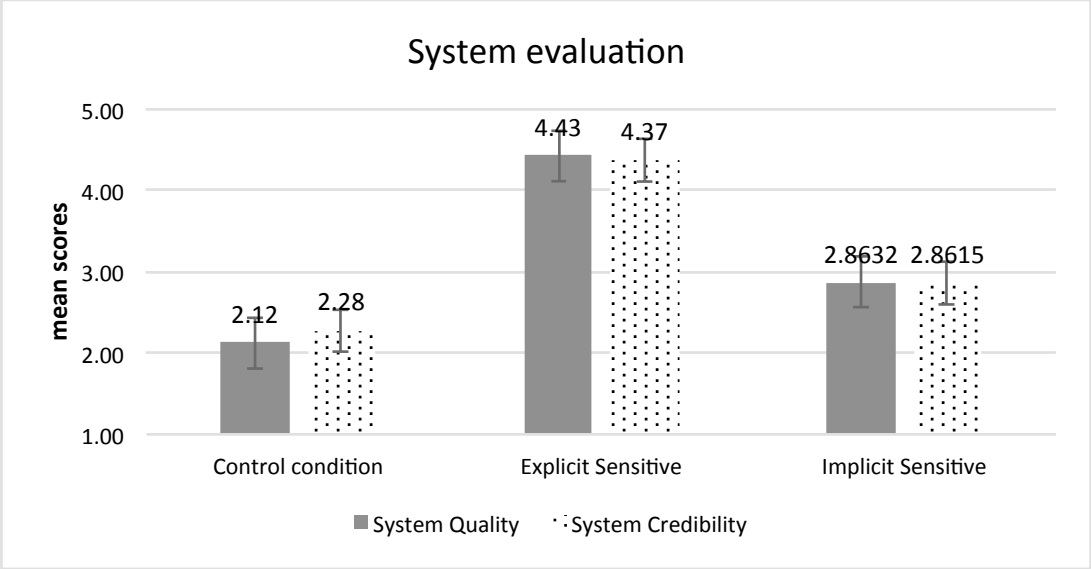

Figure 10. Mean scores of system quality and system credibility in the three conditions

Regarding the perceived sensitivity, the consolidated scores from the three items of the post-session questionnaire in the three conditions are reported in Figure 11. A univariate ANOVA was run, finding a significant effect of the condition, $F(2, 35) = 55.599$, $MSE = 27.799$, $p < .05$, $\eta 2p = .659$. The pairwise comparisons with Bonferroni correction showed that there is a significant difference between control and explicit sensitive and between control and implicit sensitive ($p<0.5$). No difference was found between the two sensitive conditions.

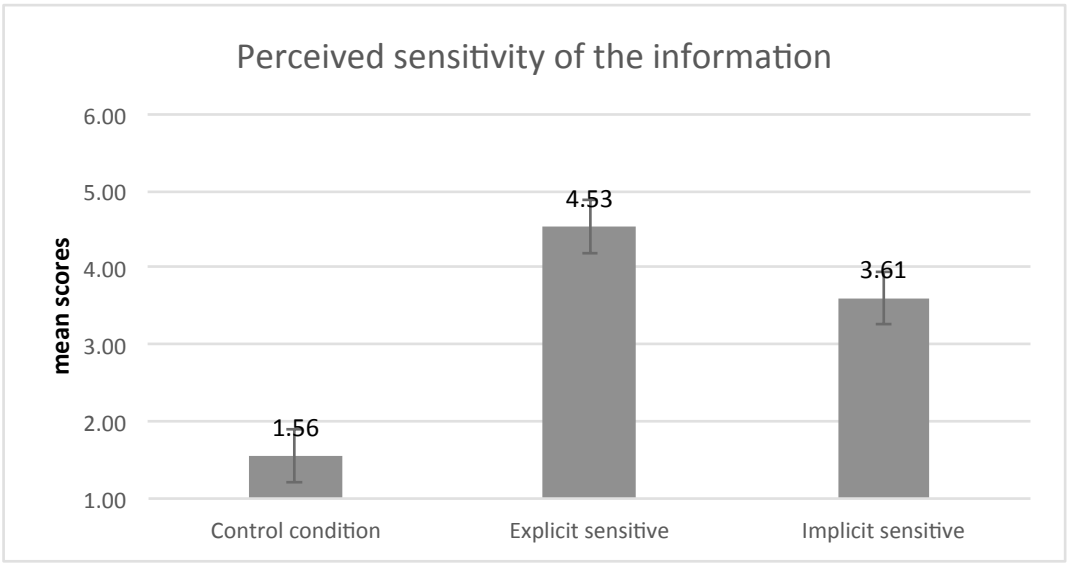

Figure 11. Mean values of perceived sensitiveness of the data provided to the system

Finally, regarding the other control variables connected to users' attitudes towards technical innovativeness and privacy, no difference was found in concern for personal privacy. A difference between the three groups was found in personal innovativeness, which resulted lower in the implicit group than in the control group, $F(2, 33) = 10.764$, $MSE = 5.38$, $p < .05$, $\eta 2p = .18$, after an univariate ANOVA was run. However since these two groups do not differ in the main dependent variable this difference is nor relevant.

3.3 General discussion and conclusions

The study found that system quality and credibility were higher after users released - for the sake of the system development – explicit sensitive information explicitly via a questionnaire. The first suggestion from this study is then that users value more a system to which they have given sensitive information, confirming out hypothesis of an effort heuristic protecting their choice retrospectively.

When sensitive data is provided implicitly instead the heuristic is not applied even though the data are considered more sensitive than in the control condition.

4 Annex III: Study 3

The goal of this study is to examine the effect of explainability of the nature of the data collected implicitly on the users' perception of the system's quality and credibility.

4.1 Method

4.1.1 Design and hypotheses

The study stems from the implicit condition used in study 2 and tests three possible variations of this conditions: no explanation of the data collected implicitly; explanation about the nature of the data; and explanation about the meaning of the data. Therefore the design includes one between-participants variable, namely data explainability, at three levels (no explanation, nature explained, meaning explained). Sensitive data in this study are, as in study 2, the participants' positive or negative opinion about his/her professors.

- *No explanation* (control condition); the participant is only given the initial instructions about the data collected with the eye-tracker, as related to the attrction/repulsion response to the professors and is ensured that the response is anonymous although in principle some physiological patterns could lead to identify a person

- *Nature explained*: in addition to the initial explanations, in this condition the participant is shown on a demo image how the eye-tracker records a path of the eye-gaze; moreover, the participant is notified - with a message on a screen - after each of the four tasks that the eye-tracker was able to recognize the position of the eye-gaze target (Figure 12). In this way the user was reminded of the nature of the data collected implicitly.

Figure 12. Notification appearing on the screen at the end of each task in the "nature explained" condition, specifying that the eye-tracker was successful in detecting the length at which the eye-gaze targeted the various images on the screen

- *Meaning explained*: in addition to the initial explanations, in this condition the participant is shown on a demo image how the eye-tracker records a path of the eye-gaze; moreover, the participant is notified - with a message on a screen - after each of the four tasks that the eye-tracker was able to recognize the responses of attraction and repulsions to the images of the professors (Figure 13). In this way the user was reminded of the meaning of the data collected implicitly.

Figure 13. Notification appearing on the screen at the end of each task in the "meaning explained" condition, specifying that the eye-tracker was successful in recording the attraction/repulsions responses to the images of the professors.

The hypotheses are the following:

H1: System evaluation in the nature explained and meaning explained conditions is higher than in the control condition.

H2: System evaluation in the meaning explained condition is higher than in the nature explained condition.

4.1.2 Apparatus

- Eye-Tracking Tobii 1700 (17" & 50 herz) (Figure 14)
- Toshiba Satellite P70-B-10T (Windows '98) to manage the calibration software of the eye-tracker and administer the forms
- Webservice "Academia Search Visualizer" of Microsoft Academic (Figure 9).

Figure 14. The Tobii monitor with eye-tracker used in the study.

4.1.3 Measures

Pre-session questionnaire

- *Demographic data*, collected via a short questionnaire before the session;
- *Familiarity* with the social network system used in the study, collected via a short questionnaire before the session and measures in a 4-degree scale (none, poor, moderate, advanced);
- *Personal Innovativeness* (Lu, Yao et al. 2005), subscales 1,2,3,4, where answers are collected on a Likert scale ranging from 1 (totally disagree) to 6

Post-session questionnaire included in this order:

- *System evaluation:* An ad hoc questionnaire composed by 19 statements about the systems' quality (Items 1 to 9 measuring the extent to which the system was readable, comprehensible, clear, graphically good, quick innovative, useful) and credibility (10 to 19 measuring the extent to which the system output was considered accurate, credible, informative, interesting, relevant, updated, objective, and the system producers were authoritative, expert), whose answers were collected on a Likert scale ranging from 1 (totally disagree) to 5.
- *Level of perceived sensitivity* of the data given, checked by three post-session items (do you think that the data collected was sensitive namely they were able to identify you counterproductively? Do you think that the data collected might be embarrassing to you? Do you fear that the data collected might be offensive to the professors?); answers were collected on a 5-degree scale were 1 meant not at all.
- *Willingness to wave anonymity warranty,* checked by two items whose answers were collected on a 5-degree scale were 1 meant not at all ("Would you let us publish your name in the credits page of the study?" and "Would you let us elaborate the data not anonymously, allowing us to associate your name and surname with the data and responses collected during the study?")

Scores of items that were formulated negatively were inverted before the analysis so that high values always mean a good perceived quality of the system.

All questionnaires were administered in electronic form.

4.1.4 Procedure

As in study 2, the participant is invited to participate in a study that aimed at collecting popularity rates of a social network in order to improve the kind of information on which the network currently is based. The goal was then to create a social network based on the popularity rates collected in the study. The study then involves a certain level of deceit and adopted several measures to protect the participant, including debriefing and a second consent to data usage after debriefing. It obtained the approval of the local ethical committee, at the University of Padua.

When the participant started the session s/he was first asked to give written consent to participate in the study. The participant was then randomly assigned to one of the conditions, was asked to fill in the pre-session questionnaire and was shown the eye-tracker component of the computer and instructed that the data on eye-gaze would be subsequently used to infer the users' response to the images of the professors in the social network graph. Then the eye-tracker was calibrated.

A printed tutorial explaining the Visualizer commands of relevance to the study was then offered to the participant. In the 'nature explained' and ""meaning explained" conditions the participant was also shown how the eye-tracker recorded the position of his/her gaze on the screen by using a demo target image. Subsequently the participants performed the tasks. They entered the query in the Visualizer, consisting of the name of one professor out of a pre-defined list of eight professors; then they had to visualize the co-author graph and write down the most common co-authors of that professor. (Professors belonged to the course in which students were enrolled and were ascertained to be present with a picture in the visualizer) In the 'nature explained' and ""meaning explained" conditions the task was followed by the notification screens displayed in Figure 12and Figure 13 respectively. The task was repeated four times, 2 times by entering the name of a male professor, and 2 times the name of a female professor.

Once the four query tasks were completed, the participant was asked to fill in the post-session questionnaire.

After the completion of the data collection of the study, participants were re-contacted, debriefed and asked for their consent to use the data.

4.1.5 Participants

The sample is constituted of 36 participants (aged 24.36 years on average, SD = 2.82), 18 women, 18 men. All participants are students or trainees at the School of Psychology, University of Padua. All participants have been assigned to one condition randomly. Eight participant declared to be moderately familiar with the social network used in the study. No difference in personal innovativeness was found in the three groups (Univariate ANOVA).

4.2 Results

The scores of system quality and credibility in the three conditions are displayed in Figure 15. The effect of information explainability on system quality and credibility was tested with a multivariate ANOVA, finding a significant effect, $F(4, 64) = 20.614$, $p < .001$, $\eta 2p = .563$. The univariate analysis showed a difference in both scores, system quality $F(2, 33) = 60{,}494$, $MSE = 12{,}906$ $p < .05$, $\eta 2p = .786$ and system credibility, $F(2, 33) = 40{,}226$, $MSE = 8{,}616$, $p < .05$, $\eta 2p = .709$. The pairwise comparisons with Bonferroni correction showed that the difference between all conditions was significant ($p<0.5$).

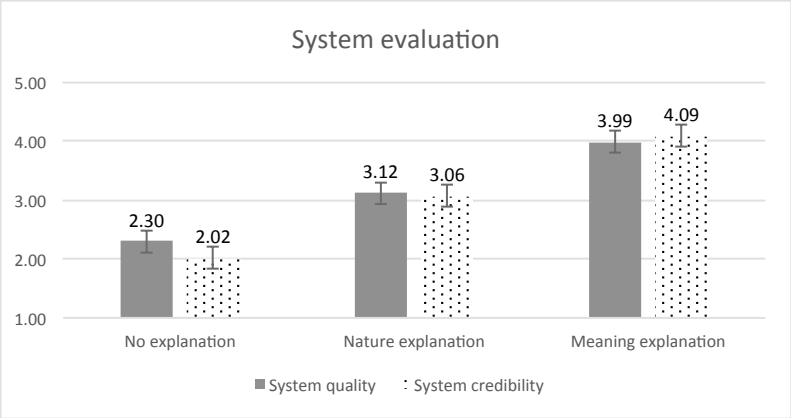

Figure 15. Mean values of the system evaluation scores in the three conditions

Regarding the perceived sensitivity of the data, as in study 2, it did not vary in the three conditions ((p> .05). However, the willingness to waive anonymity warranty seems to have decreased in the three conditions (Figure 16).

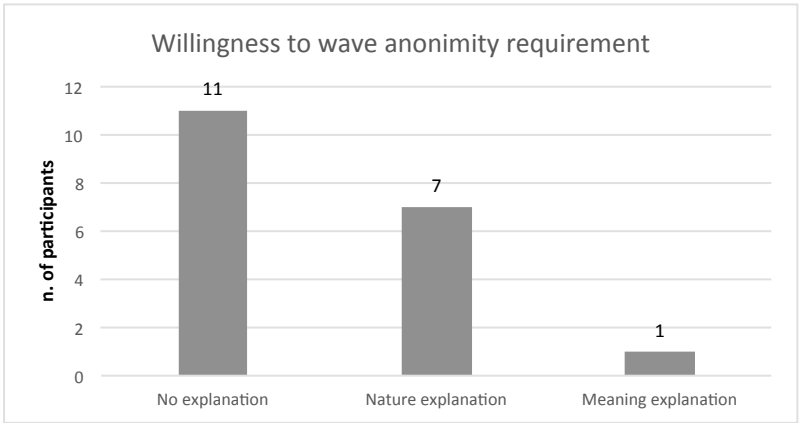

Figure 16. Number of participants willing to waive their right to remain anonymous in the three conditions (N = 12 in each condition).

4.3 General discussion and conclusions

The hypotheses were confirmed: the more transparent was the explanation of the implicit data collected, the higher was the users' perceived credibility of the system. Similarly, users' evaluation of the system quality improved as transparency increased. We interpret these results as a suggestion to improve the level of explainability of an implicit system in order to improve users' evaluation of the system and compliance with further data requests. However we raise an ethical issue regarding the defensive heuristic that might lie at the basis of such latter behaviour, which might not depend as much on the higher credibility of the system as on the increased awareness of the riskiness of the data released. This is somehow confirmed by the first study where a full transparency of the nature of the data collected in the control condition did not lead to high credibility and quality values.

5 ANNEX IV: Report from interdisciplinary panel of experts

5.1 Case 1: hidden datum.

The first case describes the use of symbiotic system where the detection of personal data for uses that are counterproductive to the unaware data owner. Indications about the realism of such a case are provided by Burgoon et al, 2003; Granhag, Vrij, Vershuere, 2015; Sartori Orru, Monaro, 2016;

"An international firm is hiring personnel in the accounting department. At the selection interview, the candidates are asked to use a pc and fill in an electronic form, collecting basic demographic information but also data about previous jobs and a description of the reasons why they think they suit the vacant position. Each candidate is also asked to sign an informed consent allowing the firm to acquire the responses to the questionnaire, which will be used for archival reasons as well as to direct the subsequent interview with the human resources manager. The form specifies that the hiring company will use the written responses to the questionnaire as well as data on the pc usage while typing the responses (time, pressure and trajectory of the mouse movements). The questionnaire is mandatory and the firm commits to keep all collected data confidential. None of the candidates is aware that data on typing behavior can be used not just to identify the user but also to detect the probability that s/he is lying."

5.1.1 Ethics

RISK: There are multiple risks involved in this case, e.g. lack of informed consent, lack of protection of best interests of the user, risk of deceit, and lack of transparency regarding data collection and data use. I suggest the area of risk involved in case 1 derives from a combination of the above mentioned risks, i.e. the system collects information about a user without informed consent or transparency for a purpose that is detrimental to the user while the benefits from such a collection belong only to the company collecting data through the system. More specifically, this represents a case of treating direct users as a 'means to an end', as mere tools to achieve the company's goal, and this would be an ethically questionable position in which to put a user. Once we can justify the use of individuals for this kind of practice – as a means to an end – the list of ethically questionable activities that may be condoned increases exponentially.

SOLUTION: A possible solution could be to mimic the current practices in aca-demic institutes whereby an ethics committee is established to monitor and approve research practices. In so doing, ethical approval has to be obtained for studies to be conducted and to provide guidance on how to do so as well as in order to protect the rights and interests of the participants involved. Outside the academy this could hap-pen on the form of an IRB for companies or an advocacy group that transcends the company as a body independent from it (i.e., not in the form of a department in the company itself). Independence is important as a way of striving for objective decisions and avoiding persuasion of ethics decisions.

5.1.2 Security

RISK: From a security perspective, the problem in case 1 is that the user provides more information than s/he means to. S/he only means to input text in the form, but in fact s/he provides a lot more information while doing so. This process, i.e., trying to use data to infer

some other information from it, is known as information leakage. There are plenty of other examples of information leakage. For example, analyzing the incoming and outgoing network traffic, the energy consumption patterns and the movement of the phone recorded when using a mobile phone, without having access to content stored on the phone, is sufficient to infer information about the user such as: the application installed on the phone, sex, age range, preferred language, text typed etc. Information leakage is a very real technical possibility, and represents a security risk because such information can be exploited in a malicious way.

SOLUTION: Despite the transaction described in this case represents such an in-fringement to several policies and users' rights that in some domains it would never been accepted (e.g., in academics), it is nonetheless a very pervasive kind of transac-tion nowadays. The use of data for extracting more information than it intended to convey by the owner of that data is technically possible and this must make as suspi-cious that such possibility is actually exploited. It would then be good to find tech-nical means to prevent such leakage to occur in the first place. The best protection in this case would be to use one's own interface to use when typing and then avoid typ-ing on other parties' interfaces. And before that I consider it necessary to increase the awareness in the user that information leakage is a likely occurrence, so they can ask for using their own interfaces in cases such as the one described in the scenario (as well as for policies, etc).

5.1.3 Law

RISK: The data collected here is used for a purpose different from the one for which it was collected; it can be considered as a deceitful use of data, and in this specific case. This kind of use could create a risk of discriminatory behavior during the recruitment process. The informed consent is insufficient, being not transparent about the use of data. The additional complication is that the collected information, in order to be used, has to be interpreted. The reliability information extracted from pc usage is also questionable and still currently under debate. Consequently, , this procedure could limitate the users' self-determination, since candidates would have behaved differently had they know the actual purpose of the data collection.

SOLUTION: I think the burden for reducing the risk is on the company, which is required (especially in the US legal system) to have a more and more "proactive" role by providing more information in the consent form thereby increasing the transparency of the process. In particular, the user should be informed that - based on evidence law where "a brick is not a wall" - the interpretation of the information about future use collected in this way (movement of mouse etc) might not be positively used by the company to inform its recruitment decisions: the reliability of interpreted information has always a margin of questionability that the user needs to be aware of (and the company alike).

5.1.4 HCI

RISK: From a human-computer interaction perspective, this case represents: 1) asymmetric value, where one side stands to gain more than the other side; 2) asym-metric risk where one side stands to lose more than the other side; and 3) asymmet-ric knowledge where one side knows what is going on while the other side does not. In a symbiotic relation the two sides are called symbiont and host. The symbiont is the company capturing and analyzing the information and the host is the user unwit-tingly providing the information. The alleged benefit for the candidate (the 'host') would be to have a chance to obtain the vacant position. Since giving data is manda-tory for the application to be considered, it can be construed as forced by the company and of value to them. For the candidate, however, it is not clear that there is any direct benefit for giving out the information. Despite this asymmetry of value this still qualifies as a symbiotic interaction. In biology, symbiotic relations do not need to be mutually beneficial to the parties involved. One can be a parasite on the other.

SOLUTION: One solution is to change the values in the asymmetry. This could be achieved by having a policy according to which people have rights over personal information. This

requires defining personal information and defining the difference between public and private domain. Personal information could be assumed to have a tier structure. When it is clear to the candidate what s/he is giving up – as determined by the tier level of private information – the company could be required to acknowledge that storing and analyzing that information is worth a certain amount. The exchange of information is then seen as a transaction which they have an obligation to pay for in some way. The candidate then would be in a position to make an informed decision whether to give up the information. If the company does not reveal the value or does not offer an appropriate amount in exchange then the candidate has grounds for a lawsuit, since whether s/he knows it or not there was a transaction and it violates the law or recognized policy concerning transactions in such cases.

A society might also decide to set a cut-off in such asymmetry, establishing for in-stance that no parasitic asymmetry is acceptable regardless of cost. That would be-come a law. Another thing to note is that in addition to the right to know a person might have intrinsic rights over future use. Since the value of a piece of information changes once it is aggregated with the information collected from several individuals it has one value in isolation and a rather greater value when part of the aggregation. If the information is now assigned a value as a function of the value of the aggregation the asymmetry of value is potentially reversed. It might even prove to be so counter-productive to the individual company to purchase information for recruitment purposes since now they would have to pay many individuals, when all they wanted was to select a few candidates. On the other hand, if there is general knowledge to be gained from this sort of data capture then a new business might spring up that provides analytic tools to companies to help them made better hiring decisions. In that case, individual companies would no longer need to capture this data and store. They could make judgements about candidates using existing analyses (sold by the new company) and throw away the data they collect themselves right after they make their decision.

5.1.5 Psychology

RISK: What in this case strikes from a psychology perspective first of all is a deficiency in informed consent. The case also points to the question of the timescale of the use of data: companies collect tonnes and tonnes of data which today are not useful, but might turn out to have a high value in the future. Logically the user cannot provide informed consent for the use of their data for a scenario or use case which today is unknown.

SOLUTION: The only approach to solving this risk is to aim for maximum Transparency: informing users of how their data might be used today (the basis of all informed consent), and also illustrating how it might be used in future. Where future uses of the data are markedly different from those envisaged at the time users consent to their data being collected, it is clear that the data collector should be required to obtain consent for the new use of the data. There are some interesting developments in this space right now, with a number of UK companies developing 'games' as part of selection and recruitment, where behaviours which are monitored during selection process game-play reveal underlying psychological characteristics of the applicant. Whilst these characteristics may be analysed with the informed consent of the applicant today, it is easy to imagine that other relationships between the game-play behavior and other psychological characteristics are discovered in the future. Without seeking new informed consent from the applicant at this point, user's test results should not be analysed for the newly discovered characteristics.

5.2 Case 2: manipulation.

The second case illustrates a scenario where a symbiotic system is used to Profiling for persuasive purposes. Indications about the realism of such a case are provided by Acar et al., 2004; or Bessi et al, 2015.

"Users of a popular search engine log in to a set of free services connected to the search engine; once they are logged-in, the computer keeps track of all webpages that are visited from the browser where the log in occurs. The search engine stores a great amount of data

about users and elaborates profiles about choices and preferences connected to the user and to similar users. In particular, it runs a free game showing several scenes and characters, recording the users positive or negative response to those characters. The search engine also runs and advertising service, which is used during a major election in one European city. The election candidate, who purchases the advertising service for the occasion, uses the stored preferences to automatically personalize the campaign ads and to make his/her portrait as a person looking as similar as possible to the individual elector. It also sends favorable voting forecasts collected from lay citizens whose profile matches the profile of the user, in terms of tastes, sports, family situation etc. Voters are positively impressed by such declarations and feel that the candidate is very close to them. The advertising firm revenue from this campaign is huge, but no money was paid to the search engine users for disclosing their information in the first place."

5.2.1 Ethics

RISK: Despite the similarities this case shares with the first one, it represents more serious threats for several reasons. In the first case the possibility that the system (of data collection and use) will be exploited for purposes that are negative for the user was questionable; in the present case such negative purposes are certain. Moreover, the negative consequences are far reaching and threaten the values at the very core of a democratic society – protection of human rights as well as undermining the democ-racy process. I would cluster two different groups of risks: 1. privacy violations and, 2. Human rights violations. For the first cluster, these violations would include: collection of data without informed consent, secondary use of data without consent, use of data for a purpose other than the one specified, possibility to de-anonymize, and lack of transparency. In the philosophical and ethical literature the definition of privacy used to focus on the control one had over one's data; deciding who has access, what is is used for, when it is used, and how much of it is used. Now, the definition of privacy has started to evolve into a concept in which the formation of one's identity is the central focus; being able to establish one's identity without having one created for you or becoming just another number. For the second cluster, the threat to human rights exists in the potential to manipulate emotions by targeting preferences and habits of users. This poses a threat to the values of autonomy and dignity of individu-als. These serious negative consequences change the nature of the scenario; the poten-tial infringement on human rights adds to the threat of the democratic process.

In deciding what to do about competing conceptions of the good life one may focus on the consequences of an action (the consequentialist approach) or the duties and principles on which the action is based (the deontological approach). Of course it is not so easy to isolate consequences from duties and many ethicists nowadays would go so far as to say that the line dividing one ethical theory from another are blurring; however, it is important in this case to be sure to point that in this case if one can attempts to justify the threat to human rights like autonomy and dignity (by undermining the democratic process) by saying that it could be a "good political candidate that is chosen", then the potential to engage in similar practices in the future with terrible outcomes (e.g. voting for a candidate or policy that is not good) becomes quite real.

SOLUTION: This is a difficult situation to find a solution for as it requires that companies and politicians are honest about their research practices even if it means they lose money. From an ethics perspective it is important to empower people to find their own voice to base their decisions on; this is why I would support education to allow people to inform their decision based on deeper knowledge of the issue. This education may come through the media or through an institution. As a solution to preventing these things from happening I would recommend establishing an advocacy group or ethics committees that work together to monitor and find solutions that make the symbiotic system process at stake ethical.

5.2.2 Security

RISK: From an information security point of view this case represents an example of user profiling. Currently, most Internet services and social networks collect data from users and try to profile them via the so-called user profiling in order to create target groups which they can target with other services (e.g., advertising) based on their characteristics. When they notify that they might sell such information to third parties, we are talking of buyers in the order of hundreds of companies what will get and use our data. While this information is commonly used in the aggregate form, it could also be exploited maliciously to try and define the profile of a specific user, his/her preferences, location and behavior. In addition the actual term of our decisions about such information is often ambiguous, as is the case when flagging as private an information on certain social media, which will never be private in the same way as we mean it to be.

SOLUTION: Increasing people's awareness of the risks involved in releasing data is nowadays necessary since security risks are chiefly underestimated. Such awareness and ability to imagine possible consequences should also be projected in the future possible use of the data which is light mindedly disclosed now. To appreciate the importance of prospective thinking we can consider DNA information sent out to Internet services in exchange for knowing something about ourselves; this equals to disclosing core identity information, information that cannot be changed and that regards not just the individual releasing such information but all his/her relatives and progeny. It is easy to imagine that such information might be used in the future for genetic research applications or discriminations we are not even aware of nowadays and that we should me more jealous of such information than other we protect with much more alacrity.

Regarding possible technical solutions, there are several and they should be better known and more pervasively implemented (the anonymous internet browser system TOR, for example). Awareness, however, is the key solutions since it will not only convince people to prefer safer solutions but also to motivate users, regulators, tech-nicians to ask for such solutions when they are not offered.

5.2.3 Law

RISK: From a legal point of view this case is about the indirect and unaware use of personal data. More technically, it is an information security law case, meaning a distinguished concept from concepts such as privacy and data security. [Many laws that purport to encourage cybersecurity are, in fact, designed with a focus on protect-ing privacy or encouraging data security]. Unlike privacy and data security, cyberse-curity is focused not only on the information, but the entire system and network. For this reason, laws that focus only on privacy and data security may not consider all factors necessary to promote cybersecurity.

SOLUTION: Transparency and adoption of best practices..

On the one hand, the popular search engine where users log in to set free services should inform users of future potential uses of their personal data through the con-nected advertising service.

On the other hand, there are also some best practices for users that can help to re-duce the risk of violation of privacy and unforeseeable use of data:

1. Anonymization: don't collect personal data if you don't need it. Work with anonymous or de-identified data if you can.

2. Disclose only the data you need and required, especially try to minimize the disclosure of sensitive personal data.

3. Encrypt sensitive personal data during transit

4. Check your contract with customers to ensure that you are not agreeing to unrea-sonable security practice in place.

Also we must consider that different kinds of information would have a different consequence in legal terms: the legal "weight" of human values and rights (e.g. reli-gion; sexsual orientation etc) is different from the legal "weight" of choices and pref-erences (e.g. kind of theatre preferences; food preferences; sympathy or not for domestic animals etc). The unware store of consumers' information about those different aspects (human rights and human preferences) have, obviously a different legal protection in case of breach. Case number 2 is important because it let stakeholders thinking about these differences.

5.2.4 HCI

RISK: I would frame this case similarly to the first case, namely as one of asym-metry in risk, value and knowledge. Unlike that case, though, this one adds a com-plication in terms of human-computer interaction, namely that there is a third party involved, and this party is not the one directly involved in the symbiotic relation. That is, the politician purchasing the service is the third party that benefits from the personal data. Presumably there was a transaction between the symbiont – the party gathering the information and the one who should have paid for it – and the politician.

SOLUTION: The system that manages collection and all transactions – the symbi-ont and its owners – has an obligation to reveal the value of the information that is being collected. This value concerns the transaction occurring between the system and the user disclosing data but especially between the system owners and the cus-tomer using the data collected. One thing is to use the collected information internally and another is to sell it. Can this information be sent to any country whatsoever? For any purpose? Its value depends on what others pay for it. So regulation should shift focus, in this case, from the transaction with the system users to the transactions be-tween the system owner and its customers who buy the collected data. Therefore, the solution would be to develop policy to regulate transactions whenever collected data are sold.

Purely from a HCI perspective, transparency can be increased by re-design, im-proving the comprehensibility by clever visualization of the meaning of terms of usage that otherwise is specified in 20 pages of text. The owner of the original information – the information host – ought to also have the right to expect to re-negotiate or renew the terms of the transaction once it is apparent the value of the information has changed. Information has a continuously changing value, it is not used once and once forever. Once new value becomes apparent there might be appropriate conditions to ask for a renegotiation. At the same time, acknowledging that some information might not be valuable once it is collected but prove valuable afterwards, it might be foreseen that its value should be paid via fee-for-use, namely only when users' data is actually used for some profit or benefit to the system owner.

5.2.5 Psychology

RISK: I think that in psychological terms this should be understood in terms of identity and individual differences, but I wonder how this case - being enabled by a symbiotic technology - differs from typical political campaigning, where politicians commonly adapt their propositions to the audience or the interlocutor.

SOLUTION: In this case, as in the first one, what is critical is to increase transpar-ency. I think that transparency in transactions - even commercial ones - should be a leading principle, allowing a better understanding of the value of the transaction. Even more so in a political domain, where democracy is at stake and there is arguably a need for even higher standards of fairness in transactions. And to achieve such transparency, I think that education of the citizen and the consumer have a huge role to play (transparency being not possibly in the absence of a user understanding what data a system is acquiring). Also relevant here is that there is a natural pressure for systems to be easy to use (to maximize likelihood of engagement) and it is likely that the user will not realize the importance of transparency of a system until s/he experi-ences some negative consequence of a lack of transparency.

5.3 Case 3: agency shift.

The third case illustrates a case where a symbiotic system might lead to Loss of agency due to automatic responses. Indications about the realism of such a case are provided by Doryab, Bardram (2011), Musen, Middleton, Greenes (2014), and by events such as the ones reported by Baum (2015).

"A hospital has adopted a laparoscopic surgery equipment which is connected to the apparatus acquiring vital signals from the patient under surgery. During the surgical procedure, the physician wears a pair of augmented reality eyeglasses to receive information about vital signals along with data about success probability for each procedure applied to the patient during the surgery, in order to better inform his/her ongoing decisions. This data is recorded for archival reasons by the hospital and can be used in case of a lawsuit against the hospital after surgeries that do not succeed. It is the hospital policy to avoid conflicts between the choice of the physician during the surgical procedure and the data displayed by the machine, the evidence of the patient status recorded by the equipment. Thus in case of the patient reaching a critical condition, the physician is recommended to only rely on the standard procedure and quit any other attempts which is less likely to succeed. Therefore, to a certain extent, the decisions are embedded in the intelligence of the computer elaborating data and making recommendations. Somehow a moral decision is incorporated into the machine."

5.3.1 Ethics

RISK: To me this represents a prototypical symbiotic relation since parts of the decisional powers are externalized by the physician to the machine based on data it re-ceives. It is a whole system including patients' data, physician's decision and systems' elaboration/recommendations. The most important part of this scenario is the fact that the surgeon is responsible for deciding whether or not he/she will take the advice of the machine. The moment this changes and the surgeon must do what the machine tells it (whether this is an explicit formal policy at the hospital or an implicit one) the scenario changes and the relation is no longer ethically acceptable or desirable. The second scenario is one in which the surgeon's freedom to choose has been limited. This limitation threatens the professionalization of medicine as one would have to be concerned about who is taking decisions and who is liable in case of problems, i.e. if the surgeon does what the machine tells it to do then will the machine be liable if someone goes wrong? Further, will we sue or fire the machine for damages? But responsibility from an ethics point of view is more than liability; it requires a moral agent with intentions who is able to reason through the consequences, understanding the consequences of an action; therefore this cannot be delegated to a machine.

Another potential risk is deskilling if the surgeon learns to rely on the technology and its elaboration more than s/he does on his/her own judgment. Moreover, with the use of this new technology the surgeon may not have an instance in which he/she is able to train using conventional methods.

SOLUTION: Using military terms, the surgeon must remain in the loop instead of being put on the loop. This means that the surgeon should be in control of giving commands and making choices. Part of the training with the systems should be to understand how the machine reasons and how to manage disagreements with the ma-chine especially during emergencies. Another part of the training should be to make sure surgeons know how to perform the surgery if/when the machine breaks and the surgeon must rely on his/her own skills without the technology (van Wynsberghe, Gastmans, 2008).

5.3.2 Security

RISK: From information security perspective this scenario points on the one hand at the aspects related to data storage in hospitals, and on the other at the possibility that the

system is programmed to make decisions, be controlled remotely or being hacked for malevolent purposes.

SOLUTION: Solutions from information security perspective for this scenario are common good practices for storage of confidential information and to make computer systems secure: avoiding unauthorized parties to take control of such systems.

5.3.3 Law

RISK: This case regards the use of extra-clinical tools to support clinical decisions.

In general the gradual shift towards the use of extra-clinical tools to supplement the informed consent process and support clinical decisions, could present the risk to consider the tool not simply support decision tool but a "replacement" decision tool (instead of the patient-physican' s decision).

Second important risk is to "blur" the principal role of physician and interfere with his freedom of therapeutic choice whose responsibility (not simply legal liability) is shared with patient.

Physicians have long faced tort liability for breach of informed consent if a patient is harmed as a result of the physician's failure to provide the information needed to make an informed medical decision. However, with increased reliance on extra-clinical informed consent mechanisms comes an increased risk of malpractice liability.

The physician who simply rely on eyeglasses without reasoning on the base of his knowledge, under even the most traditional tort principles, will be liable for malpractice. (Failure to engage fully in the informed consent process, even if decision sup-port tools are made available, is a clear breach of the standard of care).

I would invite you to think about a "What if" scenario....what if the pair of augmented reality eyeglasses give a wrong information? Similar problems where already present in the field of medical guidelines application.

Several scenarios could be traced:

1 physician follows the eyeglasses indications and he is personally persuaded by this choice;

2 physician follows the eyeglasses indications but personally he would have apply another choice;

3 physician doesn't follow the eyeglasses indications because on the base of his knowledge he would have done another choice and he decided to practice his own choice.

SOLUTION: It is clear that medical providers who prescribe or use decision sup-port tools may face tort liability if they misuse the tools or provide negligent counseling. This is a simple and relatively uncontroversial expansion of traditional malpractice liability. But the use of decision support tools also poses a secondary problem - namely, that patients may be harmed if the decision aids they use are faulty, misleading, or biased. If the regulatory or certification process aimed at ensuring the quality of decision aids fails, injured patients will look to tort law to provide a remedy. And since current tort doctrine makes it extremely difficult for such claims to succeed, it is time for policymakers and legal scholars to evaluate the costs and benefits of expanding tort liability in these cases.

The risk could be minimized with a good train and instruction by the producer on real opportunities offer by the eyeglasses. All information about the real help technology will offer to the patient should be exactly represent to the patient before the surgery in order to share "the potential scenarios".

Apart from this, it is still an open legal question in this field to determine whose responsibility is it to minimize this risk. for what we previously said, producers' will have an important role and them physician in "transfer" to the patient the useful in-formation and sharing potential scenarios prior of the intervention (learned intermediary hand role) .

Within the personalized medicine era, these eyeglasses have to be seen as a functional instrument of help in critical situation.

The risk of restricting physician's freedom of choice is inherent and it is not avoid-able. Perhaps, every physician will have to be aware that the liability for the final decision is due to his own choice, so it would be important for him to know from the producer the risk of error margin of the high tech product.

It has to be underlined that, because transitioning elements of the consent process into extra-clinical arenas is a dramatic change in the practices of protection medical freedom of choice and informed consent, it necessitates a new kind of conversation about liability. First, although product liability law sometimes subjects creators of faulty products to strict liability (that is, liability regardless of fault), decision sup-port tools do not fall within the legal definition of a "product" and so are not subject to strict liability. Their inherent autonomy is currently under analyses.

Second, in the future it will be crucial to re-analyze issues of vicarious liability of the hospital and other involved subjects.

It should be also underlined that if a hospital system requires physicians to use decision aids for particular conditions it will also have a role in the allocation of liabilities, but remember: this element will not be a "safe harbour" for physician who decided.

5.3.4 HCI

RISK: This case shows that the parties in the symbiotic relation have roles that de-pend not only on their knowledge but also on external practices such as the legal attribution of responsibility. The same case appeared years ago concerning expert systems for blood diagnosis, which were about 95% as good as a doctor on a good day. That is way better than most doctors on most days. Yet still hospitals ended up not using them because of the risk of legal suits. In normal cases gross failure leads to a law suit of the doctor. But who do you sue when it is an expert system? And what are the standards that one applies? The risk was that the responsibility for imperfection would have been laid at the foot of the programmer. And that risk might be too high given that the same program would be used in many places. The trouble is that when you think like this you give up reliable expertise (the expert system) to defend a general principle of morality or law. And yet the system is often the best way to proceed.

SOLUTION: Responsibility in this case should be allocated as a function of accountability and ultimately of knowledge. But we want humans in the loop. For instance, if an expert system left the final decision to the physician but also had a facility that would allow the physician to: a) delegate the decision to the system, on a case-by-case basis; or b) ask the system for its reasons for its suggestion or decisions and to take issue when the reasons are not clear enough, then we manage to keep hu-mans in the loop. The final decision now lies with the physician. And there is the same mechanism used among teams of humans – they talk it out by asking each other for their reasons. The system and doctor now would be a learning team.

5.3.5 Psychology

RISK: I agree with the other panellists' responses, this case reduces the surgeon's autonomy and decreases the surgeon's skills. This reminds of the same issue currently at stake with self-driving cars, where the driver must be able to deactivate the cars' automatic behavior to get in control of the situation.

SOLUTIONS: The system should be transparent, explaining itself and then allowing the surgeon to make decisions including the decision to delegate decisions.

6 References

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014, November). The web never forgets: Persistent tracking mechanisms in the wild. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Com-munications Security (pp. 674-689). ACM.

Aronson, E., & Mills, J. (1959). The effect of severity of initiation on liking for a group. The Journal of Abnormal and Social Psychology, 59(2), 177.

Baum S. (2015) Advancing smart glasses as augmented reality tool for surgeons drives Vital Medicals' capital raise. MedCityNews. http://medcitynews.com/2015/02/advancing-smart-glasses-augmented-reality-tool-surgeons-drives-vitals-medicals-capital-raise/

Benjamini, Y., and Hochberg, Y. (1995). Controlling the false discovery rate: a practical and powerful approach to multiple testing. *Journal of the Royal Statistical Society Series B* 57, 289–300.

Bessi, A., Petroni, F., Del Vicario, M., Zollo, F., Anagnostopoulos, A., Scala, A., ... & Quattrociocchi, W. (2015, May). Viral misinformation: The role of homophily and polarization. In Proceedings of the 24th International Conference on World Wide Web (pp. 355-356). ACM.

Burgoon, J. K., Blair, J. P., Qin, T., & Nunamaker Jr, J. F. (2003, June). Detecting deception through linguistic analysis. In International Conference on Intelligence and Security Informatics (pp. 91-101). Springer Berlin Heidelberg.

Cribari-Neto F, Zeileis A (2010). Beta Regression in R. Journal of Statistical Software 34(2), 1-24

Doryab, A., & Bardram, J. E. (2011, February). Designing activity-aware recom-mender systems for operating rooms. In Proceedings of the 2011 Workshop on Con-text-awareness in Retrieval and Recommendation (pp. 43-46). ACM.

Granhag, P. A., Vrij, A., & Verschuere, B. (2015). Detecting deception: Current challenges and cognitive approaches. John Wiley & Sons.

Jacucci, G., Spagnolli, A., Freeman, J., & Gamberini, L. (2014, October). Symbiotic interaction: a critical definition and comparison to other human-computer paradigms. In International Workshop on Symbiotic Interaction (pp. 3-20). Springer International Publishing.

Korzaan, M., Brooks, N., & Greer, T. (2009). Demystifying personality and privacy: An empirical investigation into antecedents of concerns for information privacy. Journal of Behavioral Studies in Business, 1, 1.

Kruger, J., Wirtz, D., Boven, L., & Altermatt, T. (2004). The effort heuristic. Journal of Experimental Social Psychology, 40, 91-98.

Langheinrich, M., Schmidt, A., Davies, N., & José, R. (2013, June). A practical framework for ethics: the PD-net approach to supporting ethics compliance in public display studies. In Proceedings of the 2nd ACM International Symposium on Pervasive Displays (pp. 139-143). ACM.

Lu, J., Yao, J. E., & Yu, C. S. (2005). Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology. The Journal of Strategic Information

Systems, 14(3), 245-268.

Musen, M. A., Middleton, B., & Greenes, R. A. (2014). Clinical decision-support systems. In Biomedical informatics (pp. 643-674). Springer London.

R Core Team (2015). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. URL http://www.R-project.org/

Sartori, G., Orru, G., & Monaro, M. (2016). Detecting deception through kinematic analysis of hand movement. International Journal of Psychophysiology, 108, 16.

Staw, B. M., Sandelands, L. E., & Dutton, J. E. (1981). Threat rigidity effects in organizational behavior: A multilevel analysis. Administrative science quarterly, 501-524.

Stekelenburg, J. J., & Boxtel, A. V. (2002). Pericranial muscular, respiratory, and heart rate components of the orienting response. *Psychophysiology*,*39*(6), 707-722

Tintarev, N., & Masthoff, J. (2007, October). Effective explanations of recommendations: user-centered design. In Proceedings of the 2007 ACM conference on Recommender systems (pp. 153-156). ACM.

van Wynsberghe, A., & Gastmans, C. (2008). Telesurgery: an ethical appraisal. Journal of Medical Ethics, 34(10), e22-e22.

