Abstract

Brain-Computer Interfaces (BCIs) are emerging technologies that acquire and translate neural data, applying that data to the control of other systems. Privacy has been identified as an ethical issue possibly arising from the use of BCIs. The research reported in this paper seeks to identify whether BCIs change privacy and if so, how and why. Interim findings are presented before outlining future research opportunities.

This paper reports preliminary data and findings from a research project that, in part, seeks to identify whether BCIs disrupt privacy. In an earlier paper, we cited and extended an existing BCI typology (Zander & Kothe, 2011) to categorize BCIs as active, reactive, passive, and hybrid (Wahlstrom et al., 2016).

- Active BCIs acquire and translate neural data generated by users who are voluntarily and intentionally engaged in pre-defined cognitive tasks for the purpose of ‘driving’ the BCI.
- Reactive BCIs make use of neural data generated when users react to stimuli, often visual or tactile.
• Passive BCIs acquire neural data generated when users are engaged in cognitively demanding tasks.
• Hybrid BCIs can be a combination of active, reactive or passive BCI, or combine an active, reactive, or passive BCI with some other data acquisition system.

Also in that paper, we analysed the four BCI types with respect to five different privacy themes and with respect to the context of BCI users (Wahlstrom et al., 2016). These analyses informed an hypothesis that reactive, passive, and hybrid BCIs are more likely to disrupt privacy than active BCIs (described below). The present paper reports preliminary findings from research designed to explore this hypothesis.

In the next section, the paper outlines the theoretical orientation of the research. This is followed by a description of the research method. Preliminary data are discussed and interim findings are presented prior to concluding with recommendations for future research.

**Theoretical orientation**

In an earlier publication we reported analysis that found conflations of privacy, security, and confidentiality may enable invalid claims of privacy protection (Wahlstrom & Fairweather, 2013). In short, when technicians conflate privacy, security, and confidentiality, they may describe security and confidentiality protections as privacy protections when, strictly speaking, few (or no) privacy protections are in place. Therefore, preventing conflation of these concepts is indicated as a key element in any technical design for supporting privacy.

Privacy, security, and confidentiality can be decoupled through consideration of social context. First, we note findings that privacy is grounded in social interaction: privacy is distinct from seclusion because it arises with respect to others (Marshall, 1972; Reay et al., 2011; Westin et al., 1979). Second, we note that security and confidentiality arise in response to motivations such as compliance with legal and professional obligations, and economic competition. Privacy is articulated by social norms grounded in social interaction. Security and confidentiality are grounded in systemic, structural practices.

Observing privacy to be socially grounded provides access to two outcomes. First, as intended, it supports the alignment of technical features to privacy discourse. Second, it suggests a theoretical orientation combining Nissenbaum’s contextual framework of information privacy (Nissenbaum, 1997, 2004, 2009) and Habermas’s Theory of Communicative Action (TCA) (Habermas, 1985a, 1985b).

Nissenbaum articulates the inter-relatedness of privacy and social context: changes in social context may give rise to changes in privacy. Emerging technologies may cause change in social contexts and consequently in privacy. In Nissenbaum’s words, “Contextual integrity reveals the systematic dependencies of social values on appropriate information flows” (Nissenbaum, 2015, p 19). The contextual framework has four key arguments, the first two of which are relevant at this point: appropriate information flows enable privacy, and appropriate information flows conform to information norms that are dependent on context. When a context is changed by emerging technology, information norms are also changed and therefore, privacy is changed.
The TCA is a theory of how systemic practices arise from and are legitimated by social norms. It is premised upon Habermas’s descriptions of the lifeworld and the system (Finlayson, 2005; Horster, 1992; H. K. Klein & Huynh, 2004; Thomassen, 2010). The lifeworld encompasses the informal, unregulated aspects of everyday life. It is shaped by, and it shapes, the attitudes and practices of people interacting in the lifeworld’s native institutions (examples include family and culture). On the other hand, the system encompasses the formal, regulated features of society (examples include law-making and economic markets). The system is dependent upon the lifeworld for its authenticity, making use of lifeworld norms to drive systemic outcomes. The lifeworld is the context of communicative actions and the system is the context of instrumental actions.

Communicative actions perpetuate the lifeworld through the sharing and ongoing adaptation of social norms; in this project, privacy norms. On the other hand, instrumental actions support systemic goals. Under the coercive influences of the system, participants in instrumental actions engage in competition and conflict, and may distort lifeworld norms in the pursuit of systemic goals. Norms distorted by instrumental actions carry the legitimacy established in the lifeworld and may be interpreted as lifeworld-authentic social norms. Thus the lifeworld is susceptible to amendment by systemic practices, for which Habermas adopts the term ‘colonisation of the lifeworld’. Habermas also argues that communicative actions replenish and perpetuate the lifeworld, providing adaptability with respect to the colonising tendencies of the system.

These theoretical orientations motivate the research method: collection and analysis of communicative actions relevant to BCI use and privacy. To clarify, Habermas’s conception of the lifeworld articulates the significance of communicative action in the mutual shaping of social norms and Nissenbaum’s contextual account of information privacy argues that emerging technologies may cause disruptions in social norms. As privacy can be articulated by social norms, the TCA and Nissenbaum’s contextual account of privacy can be accessed as theoretical scaffolds. From this, we suggest that the study of communicative actions on privacy will identify whether BCI technologies disrupt privacy norms and a research method is described in greater detail in the next section.

At this point, two clarifications are important. The first regards terminology and the second regards various themes in the privacy research literature.

As to terminology, we use the term *disrupt* to avoid the negative bias inherent to terms such as privacy *violation*, *loss*, or *leakage*. We considered using the term privacy *change* however it fails to indicate the pace of privacy disruption in the context of emerging technologies. *Change* also fails to indicate the scale of privacy disruption. That is, *change* can be interpreted as confined to one concept whereas *disruption* is more readily understood as having a wider effect, as suggested in studies of user behavior with respect to privacy (Fuster, 2010). While pace and scale are relevant, we intentionally leave open the question whether privacy disruptions carry intrinsic negative connotations. Instead, we aim to understand privacy disruptions and we await the analysis of further data before forming an argument and drawing conclusions.

As to various themes in the privacy research literature, in a previous paper we reviewed research literature on privacy and found five privacy themes, which are very briefly stated here
The control theme suggests that people like to control the data that describes them (Westin, 1970). The restricted access theme argues that control is infeasible in the context of contemporary technologies and therefore regulation to restrict access to personal data is called for (Gavison, 1980). The commodification theme suggests that personal data is an alienable commodity that may be traded (Schwartz, 2004). The contextual theme has been outlined above: privacy and social context are co-related (Nissenbaum, 2009). Finally, the ontological theme suggests that personal data is intrinsic to a person in the way that feelings are intrinsic (converse to the commodification theme) and privacy is a function of traction in the infosphere (Floridi, 2005). These diverse privacy themes are relevant to this project for two reasons. First, the themes arise in the privacy literature and are therefore legitimized by, and of interest to, the research community. Second, the diversity of these privacy themes will enable research participants, who are likely to be laypeople with respect to the privacy literature, to engage in relevant, detailed, and broad discourse.

**Method**

This research project uses an experimental format aiming to address two research questions, the second of which is dependent upon the first.

1. Do BCIs disrupt privacy?
2. If so, how?

If the answer to the first research question is *yes* there may exist a requirement for a technical intervention to support privacy. The answer to the second question will explore the ways in which privacy is disrupted and in doing so, identify whether a particular technical intervention is suggested and inform its design.

An earlier paper (Wahlstrom et al., 2016) hypothesized potential privacy disruptions; these hypothesized disruptions are reproduced in Table 1. Twenty distinct Privacy-BCI domains exist, from the Control-Active domain to the Ontological-Hybrid domain. Three user groups were considered relevant: compelled users, coerced users, and all users. ‘Compelled users’ willingly use a BCI, although they are compelled by circumstances beyond their control, for example, users with impairments who benefit from using a BCI. ‘Coerced users’ unwillingly use a BCI, for example, users who are under interrogation. ‘All users’ designates all other users and compelled users and coerced users. Hypothesized privacy disruptions for compelled and coerced user groups represent special cases, whereas privacy disruptions for all users are generic.

Communicative actions reveal privacy norms and are therefore an important component of this research. The first research question is addressed by comparing an initial privacy norm (the control) to a subsequent privacy norm (the dependent), both of which are articulated in the communicative actions of small groups of participants. Between each communicative action, individual participants use an active BCI (the condition) to establish experiential knowledge of the technology’s capabilities. These research activities are now described in greater detail.

Participants are selected according to two criteria. Firstly, as the project’s hypothesis consists of twenty distinct Privacy-BCI domains, each at the intersection of a privacy theme and a BCI type,
it is required that participants have the capability to comprehend thematic and technical distinctions, and be able to make and articulate nuanced observations. Therefore, participants are recruited from the research student community at the corresponding author’s home institution. Secondly, as the experiment sets out to measure the extent to which privacy norms are influenced by BCI familiarity, it is required that participants have no prior experience of BCI technology.

The project’s method consists of two phases: the pre-selection survey followed by communicative actions.

The pre-selection survey was adapted from the Office of the Australian Information Commissioner’s privacy attitudes survey, with permission (Office of the Australian Information Commissioner). It has three sections: demographics, privacy attitudes, and communicative competency. The demographic data enables small groups to be formed such that demographics neither hinder nor unduly influence communicative actions. The privacy attitude data will enable small groups to be formed such that diverse privacy attitudes are represented in each small group. The communicative competency data will support discourse analysis. So far, the pre-selection survey has attracted 31 respondents. Interim data are presented and analysed in the next section.

Participants for the communicative actions are selected from respondents to the pre-selection survey. Participants are sorted into small groups so that privacy attitudes and academic disciplines are mis-matched. Mis-matched privacy attitudes are an experimental pre-condition because such attitudes are more likely to give rise to communicative actions. Mis-matched scholarly disciplines are an experimental pre-condition to ensure diverse bodies of knowledge are brought to the communication actions.

In order to establish familiarity with each other, the small groups share lunch, engage in some ice-breaking and grant informed consent prior to commencing the four research tasks described below. It is important participants establish personal familiarity in order to ensure discursive actions are genuinely communicative rather than instrumental. The more participants know each other and understand the goal of their discursive actions, the more communicative and less instrumental these actions are likely to be. After lunch, ice-breaking, and granting informed consent, small group participants complete four tasks.

The first research task requires a group to engage in a guided communicative action in order to establish the group’s privacy norm. As participants’ privacy attitudes are diverse, a group’s privacy norm may range from “we hold irreconcilable views on privacy” to a specific and detailed group privacy norm.

In the second task, individual participants observe the reliability and scope of BCI technology as it acquires, interprets and applies their thoughts. Participants use an Emotiv EPOC BCI. This is an active BCI consisting of an EEG headset and a software package with two main components. The first component is a machine-learning module that matches a specific neural pattern to a specific intention. The second component reads, interprets, and applies a participant’s neural patterns as they deliberately attempt to manipulate an object on the screen. Built-in manipulations are neutral, push, pull, up, down, rotate left, rotate right, and disappear. A
participant wears the EPOC headset and observes their baseline EEG readings. Then, the BCI learns to recognize the participant’s neural activity for the neutral and push manipulations, and then the user controls the user interface of the BCI, executing the neutral and push manipulations by thinking. Figures 1 and 2 are screen captures of the BCI technology depicting a user executing the neutral and push manipulations. Participants use the BCI until they are ready to stop, training the BCI and attempting various manipulations according to preference.

In the third task, individual participants complete a de-briefing interview in which they consider the four different types of BCIs through the lenses of the five privacy themes. In order to support participants’ observations, cards are used. A set of five cards designates the five privacy themes and a set of four cards designates the four types of BCI. A card from each set is combined with a card from the other set until all twenty combinations have been considered. For example, the control privacy theme is paired with passive BCI in order to elicit privacy disruptions for this domain. Participants construct a map with descriptions of privacy disruptions.

As the second and third tasks are completed individually, small group participants not engaged in these tasks are free to spend the time as they wish, although not in each other’s company. This condition exists to prevent participants from prematurely comparing their analyses of privacy disruptions.

Finally, in the fourth task, the small group re-convenes to repeat the communicative action and re-establish the group’s privacy norm. During this communicative action, participants may refer to their own descriptive maps of privacy disruptions.

Communicative actions and de-briefing interviews are voice-recorded and will be transcribed before analysis. Each small group constructs two privacy norms: the control and the dependent. The dependent will be compared to the control to determine whether BCIs disrupt privacy. Should this be the case, discourse analysis over both communicative actions and over individual participants’ interview data will explore the ways in which privacy is disrupted in order to ascertain whether a technical intervention is suggested and should it be, to inform its design.

**Analysis**

The research method has features of both quantitative and qualitative research traditions: an evaluation of pre-selection data enables interpretive analysis of discourse arising in communicative actions. Discourse analysis depends upon data that is deeper rather than broad, with fewer participants providing highly detailed data. For this reason, the number of participants need not be as high as would be required for a strictly quantitative study.

An interpretive analysis of discourse will complement analyses under Habermas’s TCA and Nissenbaum’s contextual framework. It is proposed that discourse data arising from the communicative actions be analysed under these three theoretical lenses. In this way, findings from complementary analyses may be contrasted.
Habermasian discourse analysis applies three validity criteria: truth (Wahrheit), rightness (Richtigkeit), and authenticity (Wahrhaftigkeit). Truth relates to a concept’s factual integrity; rightness relates to its consistency with established social norms; authenticity relates to the extent to which the participant’s discussion represents the concept. The validity of a discourse can be established with reference to these criteria. In this project, the validity criteria can be applied to the communicative actions through which small groups establish privacy norms in order to articulate and contrast validities.

Nissenbaum’s contextual framework is comprised of four arguments: appropriate information flows enable privacy; appropriate information flows conform to information norms that are dependent on context; these contextual information norms consist of five elements (data subject, sender, recipient, information type, transmission principle); privacy arises from ethical concerns that change over time. Thus, identifying the five elements of a contextual norm is key to identifying whether an information flow is appropriate. In this project, the communicative actions establishing privacy norms will be analysed with a view to identifying these five elements in order to establish the appropriateness of information flows.

As the research method will produce several privacy norms and the Habermasian discourse analysis may enable the validity of these norms to be established, it will be possible to compare the contextual appropriateness of a privacy norm with its Habermasian validity. This analysis will contribute a novel perspective on the extent to which these theories can be reliably merged.

In addition to this exploration of theoretical terrain, an interpretive analysis will be conducted. This analysis will identify and codify important themes and variations in the text, enabling an argument responding to the second question to be constructed from communicative action discourse.

Interim findings

At the time of writing this paper, the first and second phases are ongoing; at the time of presenting the paper, the first phase will be complete and the second phase will be ongoing. There were 31 respondents to the pre-selection survey and demographic data including sex, age, and number of dependents are presented in Table 2. 8 cultural groups (see Table 3) are represented, with two respondents providing erroneous responses (“n/a” and “Caucasian”); 10 academic disciplines (see Table 4) are represented, with one respondent providing an erroneous response (“PhD”). None of the respondents have used a BCI in the past and 29 consented to receive an invitation to participate in phase 2.

A pilot group of 3 participants has been formed so that the research protocol and instruments may be calibrated, after which it will be possible to form 5 groups of 5 participants, or up to 8 groups of 3 and 4 combination thereof. As noted in the discussion on method, pilot group participants are mis-matched on privacy attitude and academic discipline. Pre-selection survey responses on privacy attitudes have been scored and normalized to a range of 0-100. Privacy attitude scores are summarized in Table 5. Lower scores indicate a more lassez faire attitude to privacy than higher scores, which indicate privacy awareness and sensitivity.
There are two interesting features in the empirical data on privacy attitude. Firstly, only Australians have privacy scores 31-40 range, although there are Australians in other ranges. Secondly, the respondent with the highest score (78.38) also has the greatest number of children. However, as N =31 these interim findings have no statistical significance.

More importantly, the privacy scores have enabled a pilot group to be formed. As participants in small groups are to represent diverse privacy attitudes, the pilot group was formed using a 4-step process that ensured diverse privacy attitudes for all groups. First, pre-selection participants declining invitations to participate in Phase 2 were removed from the data. Second, the participant providing the erroneous response on cultural background was removed from the data. At this point, 28 pre-selection respondents remained. Third, privacy scores were sorted from lowest to highest. Finally, to be consistent with the research method, participants were selected so that privacy scores and academic disciplines were mis-matched. The privacy scores and academic disciplines of the pilot group are presented in Table 6.

Other characteristics of the pilot group are that all participants are male; two participants have dependents; two participants are in the 35-54 age group and one participant is in the 25-34 age group; participants are from diverse cultural backgrounds (African-Australian, American, Bangladeshi). At the time of writing, the pre-selection survey remains open and the pilot group is scheduled to complete the phase 2 research tasks.

**Conclusions**

This paper outlines a research project for identifying whether BCIs disrupt privacy and, if so, how. It commences with an observation that decoupling privacy from security and confidentiality supports closer alignment of privacy and technical designs, and achieves this decoupling by viewing privacy as a social norm and security and confidentiality as systemic. This view of privacy enables access to Habermas’s TCA and Nissenbaum’s contextual framework for information privacy as theoretical foundations: the TCA articulates the significance of communicative action in the mutual shaping of social norms and Nissenbaum’s contextual account of information privacy argues that emerging technologies may cause disruptions in social norms. Thus, social norms relating to privacy form the subject matter of the research and BCIs provide the environment.

In order to identify whether BCIs disrupt social norms relating to privacy, a research protocol in two phases was described. The first phase is a pre-selection survey and the second consists of four tasks aiming to reveal privacy norms for study and analysis; participants complete a communicative action in a small group, establish knowledge of BCI technology and de-brief as individuals, and complete a second communicative action in the small group. The communicative actions enable groups to articulate two privacy norms: prior to establishing knowledge of BCI technology (the control) and after (the dependent). Comparing the two privacy norms will provide an opportunity for considering whether BCIs disrupt privacy. Should privacy be disrupted by BCI technology, a technical intervention may be advantageous. Interpretive analysis of the discourse arising in the communicative actions and the de-briefing data may provide insight as to how the disruption arises and therefore, may inform the design of a technical intervention. The data collection is ongoing and future research tasks will calibrate
the research instruments, analyse data to establish findings, and, if required, design a technical intervention.

A second opportunity arising from this research is the capacity to consider the research project’s theoretical foundation. Contextual appropriateness of privacy norms will be established by applying a discourse analysis informed by Niseenbaum’s contextual framework, whereas the Habermasian validity of the privacy norms will be established through analysis with respect to the truth, rightness and authenticity validity criteria. Therefore, this research presents a unique opportunity to contrast these two perspectives and then make suggestions on methodological adaptations for future research into technology and privacy.

Acknowledgements

The introduction section of this paper is adapted from Wahlstrom & Fairweather (2013).
References

Allison, B., Wolpaw, E., & Wolpaw, J. (2007). Brain-Computer Interface Systems: progress and prospects. Expert Review of Medical Devices, 4(4), 463-474.

Bonaci, T., Calo, R., & Chizeck, H. (2014). App stores for the brain: Privacy & security in Brain-Computer Interfaces. Paper presented at the IEEE International Symposium on Ethics in Science, Technology and Engineering.

Farah, M. J., & Wolpe, P. R. (2004). Monitoring and Manipulating Brain Function: New Neuroscience Technologies and Their Ethical Implications. The Hastings Center Report, 34(3), 35-45.

Finlayson, J. (2005). Habermas: A Very Short Introduction: Oxford University Press.

Floridi, L. (2005). The Ontological Interpretation of Informational Privacy. Ethics and Information Technology, 7(4), 185-200.

Fuster, G. (2010). Inaccuracy as a privacy-enhancing tool. Ethics and Information Technology, 12(1), 87-95.

Gavison, R. (1980). Privacy and the Limits of Law. The Yale Law Journal, 89(3), 421-471.

Goering, S., & Yuste, R. (2016). On the Necessity of Ethical Guidelines for Novel Neurotechnologies. Cell, 167(4), 882-885.

Habermas, J. (1985a). The Theory of Communicative Action, Volume 1: Reason and the Rationalization of Society: Beacon Press.

Habermas, J. (1985b). The Theory of Communicative Action, Volume 2: Lifeworld and System: A Critique of Functionalist Reason: Beacon Press.

Horster, D. (1992). Habermas: an introduction: Pennbridge.

Klein, E., & Nam, C. S. (2016). Neuroethics and brain-computer interfaces (BCIs). Brain-Computer Interfaces, 3(3), 123-125.

Klein, H. K., & Huynh, M. Q. (2004). The critical social theory of Jürgen Habermas and its implications for IS research. In J. Mingers & L. Willcocks (Eds.), Social theory and philosophy for information systems: Chichester: Wiley.

Li, Q., Ding, D., & Conti, M. (2015). Brain-Computer Interface applications: Security and privacy challenges. Paper presented at the IEEE Conference on Communications and Network Security (CNS). http://dx.doi.org/10.1109/CNS.2015.7346884

Marshall, N. (1972). Privacy and Environment. Human Ecology, 1(2), 93-110.

Nissenbaum, H. (1997). Toward an Approach to Privacy in Public: Challenges of Information Technology. Ethics & Behavior, 7(3), 207-219.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review, 79(1), 119-157.
Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life: Stanford Law Books.

Nissenbaum, H. (2015). Respecting context to protect privacy: Why meaning matters. Science and engineering ethics, 1-22.

Office of the Australian Information Commissioner. Community Attitudes to Privacy. Retrieved December 20 2016, from http://www.oaic.gov.au/engage-with-us/community-attitudes/  

Reay, I., Beatty, P., Dick, S., & Miller, J. (2011). Privacy policies and national culture on the internet. Information Systems Frontiers, 13(5).

Schwartz, P. (2004). Property, Privacy, and Personal Data. Harvard Law Review, 117(7), 2056-2128.

Thomassen, L. (2010). Habermas: a guide for the perplexed: Continuum.

Wahlstrom, K., Fairweather, B., & Ashman, H. (2016). Privacy and Brain-computer Interfaces: Identifying Potential Privacy Disruptions. SIGCAS Comput. Soc., 46(1), 41-53.

Wahlstrom, K., & Fairweather, N. B. (2013). Privacy, the Theory of Communicative Action and Technology. Paper presented at the ETHICOMP, Kolding, Denmark.

Westin, A. (1970). Privacy and Freedom: Bodley Head.

Westin, A., Sentry Insurance, S. P. W. I., Harris, L., Associates, I. N. Y. N. Y., & Others. (1979). The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy.

Zander, T., & Kothe, C. (2011). Towards passive brain–computer interfaces: applying brain–computer interface technology to human–machine systems in general. Journal of Neural Engineering, 8(2), 025005.

Table 1

Hypothesized privacy disruptions.

| Privacy theme | BCI type       | Pa      | Hy      |
|---------------|----------------|---------|---------|
|               | Active         | Reactive|         |
| Control       | Compelled users| All users and Coerced users | All users |
| Restricted    | All users      | All users| All users |
| access        | Commodification| All users| All users |
| cation        |                |         |         |
| Contextual | Compelled | All users and Coerced | All | All |
|------------|-----------|------------------------|-----|-----|
| users      | users     | All users              | All | All |

| Ontologica | All users | All users | All | All |

I

Users

Users
Table 2

Sex, age group, and dependents.

| Trait       | % of respondents |
|-------------|------------------|
| Female      | 32               |
| Male        | 68               |
| Age: 18-    | 19               |
| Age: 25-    | 48               |
| Age: 35-    | 32               |
| Depend ents: 0 | 71          |
| Depend ents: 1 | 16          |
| Depend ents: 2 | 10          |
| Depend ents: 3 | 3           |
| Depend ents: 4 |             |
Table 3

*Cultural backgrounds.*

| Cultural background                                      | % of respondents |
|---------------------------------------------------------|------------------|
| African-Australian / Anglo-Australian                    | 28               |
| Australian                                              |                  |
| Bangladeshi / South Asian / Sri Lankan                  | 14               |
| Cambodian / Indonesian / Malaysian                      | 14               |
| Vietnamese                                              |                  |
| Iranian or Persian / Palestinian                        | 14               |
| Asian / Chinese                                         | 14               |
| English / Italian                                       | 10               |
| American                                                | 3                |
| Russian                                                 | 3                |
Table 4

Academic disciplines.

| Disciplines                                                        | % of respondents |
|-------------------------------------------------------------------|------------------|
| Engineering / Mechanical Engineering / Mechatronic Engineering     | 1                |
| Computer Science / IT                                             | 8                |
| Health Science / Psychological Science / Psychology / Population Health | 4                |
| Education                                                         | 1                |
| Environment Science                                               | 7                |
| Linguistics                                                       | 7                |
| Management                                                        | 7                |
| Physics / Sciences                                                | 7                |
| Law                                                               | 4                |
| Transport Planning                                                | 4                |
Table 5

*Privacy attitude scores.*

| R | %   | of respondents |
|---|-----|----------------|
| 3 | 6.45|                |
| 1-40 | 19.35|                |
| 4 |     |                |
| 1-50 | 45.16|                |
| 5 |     |                |
| 1-60 | 19.35|                |
| 6 |     |                |
| 1-70 | 9.68 |                |
| 7 |     |                |
| 1-80 |     |                |
Table 6

Pilot group experimental pre-conditions.

| Privacy score | Academic discipline |
|---------------|---------------------|
| 53.67         | Transport Planning  |
| 63.32         | Management          |
| 78.38         | Physics             |
Figure 1. Neutral

Figure 2. Push