# eFRIEND: an Ethical Framework for Intelligent Environment Development

Simon Jones, Sukhvinder Hara, Juan Augusto

Department of Computer Science
Middlesex University
The Burroughs, Hendon
London NW4 4BT

## ABSTRACT

Intelligent Environments bring technology closer to daily life and aim to provide context-sensitive services to humans in the physical spaces in which they work and live. Some developments have considered the ethical dimension of these systems; however this is an aspect, which requires further analysis. A literature review shows that these approaches are rather disconnected from each other, and that they are not making an impact on real systems being built. This paper summarises the ethical concerns addressed by previous work, highlights other important concerns, which have been overlooked so far, and proposes a more holistic approach. It explains how these concerns can be used to guide part of the development process in such a way that Intelligent Environments being engineered in the future will consider the ethical dimension in practice, not just in theory.

**General Terms**

Security, Human Factors, Standardization, Theory, Legal Aspects

**Keywords**

Intelligent Environments, Privacy, Data Protection, Security, Transparency, Autonomy, Multi-User Environments, User-Centric, Ethical Principles and Frameworks.

## INTRODUCTION

*Intelligent Environments* is an area of recent development, and one that shares substantial concepts and objectives with several other fields of recent emergence, such as *ambient intelligence, pervasive* and *ubiquitous computing*, and *ambient assisted living* (Augusto et al, 2013a). Intelligent environments are built to assist users to be independent whilst monitoring their state for a variety of conditions. They utilise a range of embedded devices, sensors, biometrics and wearable technology.

This paper looks at the extent to which social and ethical issues have been addressed in the existing literature. We identify the main ethical concerns addressed by previous work as well as highlighting the relevance of other concerns, which are important but have been overlooked so far. These issues are summarised in section 2 below. Section 3 focuses on those papers that present a framework for addressing ethical issues. A comparative analysis of these found disparity amongst them, and, especially concerning for teams developing real systems in this technical area. Our aim is to translate those findings / key ethical principles into practical action / a methodology which can transform the discussion at a conceptual level into a real benefit for society. With this in mind, a new, more practical, system is proposed in section 4, one that includes elements of the existing frameworks that we have surveyed, but also extends them into the engineering process of creating actual systems. Our method has been validated by an EU funded research and development inclusion project, *POSEIDON*. [Augusto et al, 2013b).

# SURVEY OF ETHICAL ISSUES

Privacy is perhaps the single ethical issue of greatest concern in relation to intelligent environments and by far the most frequently cited issue in the literature surveyed. Concerns about privacy flow from the large amounts of personal data that are collected, distributed and exchanged in such systems (Aarts, 2004; Wright et al, 2010; Ikonen et al, 2009). Friedewald et al suggest that AmI increases the amounts of detailed personalized data that is collected, distributed and stored, much of which is sensitive medical and identification information (Friedewald et al 2005). This allows decisions to be made on the collected data (Bohn et al, 2004). Van Heerde et al (2006) for example, note that it is the both high quality and large quantities of data that can be collected that enable the intelligence of AmI systems, whilst providing privacy challenges, which has the potential for misuse/abuse of this sensitive information (Friedewald, 2005; Schülke et al, 2010). Wright et al (2010) argue that ambient intelligence technology violates most existing privacy-protecting borders. Increased connectivity between people and spaces blurs physical borders such as walls and doors together with remaining always connected, also acknowledged by Chan et al (2009) as one of the major inhibitors to the adoption and implementation of smart homes.

However, the findings from various projects, with potential user groups, are by no means uniform. Coughlin et al, for example, found that ageing service providers and policy advocates had ethical considerations for trust and privacy issues, 24/7 home monitoring and third party use of behavioral data by commercial entities, such as marketing or insurance companies (Coughlin et al, 2007). However, Van Hoof et al (2011) found that older respondents were *not* worried about privacy-related issues, and did not feel watched or monitored but benefits outweighed concerns (postponing of institutionalisation) afforded by ambient intelligence technologies.

Following on from these privacy concerns, a number of authors have highlighted specific data protection issues. These include the storage and retention of personal data, access to such data, by third parties, and the risks of disclosure of sensitive data (Sadri, 2011). This raises issues of confidentiality, trust and informed consent (Sliwa & Benoist, 2011; Wright et al, 2010) and whether the amount and detail of personal information requested in the design of such systems is proportionate to their operational needs (Sadri, 2011).

Another set of concerns are the remote monitoring and surveillance capabilities of these technologies through various sensors. Permanently networked technologies has brought with it new surveillance issues for ethical architectural design according to Albrechtslund (2007). A number of authors have accordingly raised the spectre of a "big brother" society where it will be increasingly difficult to be left alone (Schülke et al, 2010; Wright et al, 2010) and the *feeling* of being under surveillance Langheinrich et al (2004). Similar concerns are raised about safety and security of intelligent environments (Aarts, 2004; Nixon et al, 2004; Van Hoof et al, 2007; Rashidi, 2012), and a trade-off between security/safety and privacy is recognised (Landau et al, 2010; Sharkey and Sharkey, 2012).

AmI systems are, generally, *distributed* systems in which multiple artificial and human agents collaborate and interact. As artifacts become more autonomous and make human intervention unnecessary, the question arises of who is responsible if things go wrong and with whom legal liability rests with? (Langheinrich et al, 2004, Bohn et al, 2004). If the objective of smart environments is invisible technology and natural interaction, do those technologies and interactions have to be made less invisible and less natural in order to answer users' concerns, about privacy, for example? This perhaps is overlooked due to commercial pressure (Augusto, J.C., McCullagh, P.J., Augusto-Walkden 2011).

Equality of access to technology is another key ethical issue that intersects with broader questions about the digital divide. Wright et al (2010) and Bohn et al (2004) question whether AmI technology will be universally and equally available to all potential users, or only to those who can afford them, exacerbating inequalities Brown and Adams (2007). The incorporation of user perspectives into design and development is widely recognised as one of

the foremost challenges in creating effective assistive technologies (Oishi et al, 2010; Van Hoof el al, 2011; Rashidi, 2012). From this literature review, we identify the following seven key areas, around which ethical and social issues are clustered: - ***Privacy, Data Protection, Security, Transparency, Autonomy, Equality and Dignity***.

# REVIEW OF ETHICAL FRAMEWORKS

This section examines those articles from the literature surveyed, which propose a framework for addressing ethical issues. Common foundations for some of these frameworks are principles drawn from the field of medical ethics, in particular those proposed by Beauchamp and Childress (2001). This framework consists of four major principles: - *Autonomy*, *Beneficence*, *Non-maleficenc*e and *Justice*, which have been applied by Schulke et al (2010) and Perry et al (2009). Schulke et al (2010) propose a hierarchy of ethical principles as follows: - *Non-harm, Autonomy, Welfare Provision and Equality.*

Coeckelbergh (2010) argues that whilst privacy is an important issue, it is not the *only* one, or even the most important one. Other healthcare principles, such as the capabilities outlined by Nussbaum (2006) and that include preservation, restoring, maintenance and enhancement of life, dignity, bodily health and bodily integrity. Ikonen et al (2009) propose a framework of six principles in their project to design a mobile phone platform for ambient intelligence applications. These principles were complemented with issues identified by user groups. A set of six ethical guidelines were generated from this process: - *Privacy, Autonomy, Integrity and dignity, Reliability, E-inclusion and Benefit to society.*

Callaghan et al (2009) categorise intelligent agents in terms of two underlying approaches; *end-user programming* (which empowers the user) and *autonomous-agent programming* (which reduces the cognitive load placed on the user, but involves less transparency). Callaghan argues that the less understanding of, and control over, their technological environment that people have, the more resistant or fearful they will be of it (resulting in technophobia). Ball and Callaghan's research into users' views about intelligent environments suggests that maintaining control or autonomy is a paramount concern, in terms of the freedom of users to make choices for themselves (Ball and Callaghan, 2011).

While there are many useful elements in these various frameworks, a comparison of the main ethical principles discussed by them reveals considerable disparity in coverage of the seven major themes identified above. They incline to be either philosophical or prescriptive at a conceptual level and tend to look at ethical issues in isolation from the practical process of designing and engineering systems themselves. Lastly, they tend to assume a single primary user, whereas, in reality, most systems are likely to be implemented in a *multi-user* environment.

We propose a more holistic framework, which arguably has a greater chance of impacting favourably on the real world by immersing ethics in the engineering process of creating real, multi-user systems. We outline a methodology, which enables ethics to be embedded in the core of any system.

# eFRIEND FRAMEWORK

While each of the frameworks discussed above have their respective merits, we propose an alternative, more comprehensive, framework that combines their best elements with principles drawn from our own experience of engineering systems in this area. These principles are informed by the *Intelligent Environments Manifesto* proposed by Augusto et al (2013a) that advocates the development of systems in a manner which is aligned with a number of explicitly defined priorities. In particular we espouse the following principles: -

- P3—deliver help according to the needs and preferences of those who are being helped
- P5—preserve the privacy of the user/s
- P6—prioritize safety of the user/s at all times

- P9—adhere to the strict principle that the user is in command and the computer obeys

We propose the following user-centred principles, which we consider fundamental to empower users of intelligent environment systems. Firstly, ***non-maleficence*** and ***beneficence*** should be considered as general principles that should inform the entire development process. We understand non-maleficence, as the principle of not developing any system that will cause harm, particularly to primary users. *Beneficence*, we understand, as the principle of working for the social benefit of users, by increasing their quality of life and, more broadly, for society generally.

Our approach is also fundamentally ***user-centred*** whereby the views of various stakeholders, particularly the users should be a central consideration throughout all the stages of any project. We prioritise the need to identify and accommodate the preferences and requirements of ***multiple user groups*** and stakeholders in any number of different settings. Potential stakeholders to be considered include; *primary users* [who may be individuals with complex social and health care needs]; *secondary users* [family members, carers and professionals] working in a range of settings; and *tertiary users* [those from a broader spectrum of services].

In terms of the seven specific ethical principles outlined in the previous section, we stress the issue of ***privacy***. We argue that privacy settings and options need be taken into account, and designed into any system, from the beginning of the development process. Crucially important is the users' ability to exercise control over monitoring, tracking and recording activities in intelligent environments, and over the information capture and dissemination capabilities of any such environments. Emphasis is placed on user ability to specify and adjust privacy levels for different services. We regard the communication of privacy risks to potential users as a priority, as well the ability of both primary and secondary users to convey their own privacy requests and preferences to appreciate the privacy implications of disclosing personal information about themselves together with obtaining informed consent for any data processing or monitoring as important.

Personal information that is collected and processed from any intelligent environment must comply with relevant ***data protection*** legislation, both in principle and practice, as well as data accessibility, accuracy, relevance and appropriate use. Users should be able to determine the level of information sharing between tertiary users, and to specify what personal data can be accessed, and how it can be used and further disclosed by explicit consent. In multi-user environments this implies being able to effectively distinguish between personal data for various different purposes, such as health monitoring or user of commercial services. We regard the building into any system of adequate and appropriate s***ecurity*** to be an ethical and professional responsibility, and a key foundation of user trust and confidence in any intelligent environment. Specially maintaining safety and security for data collected, processed, stored particularly with wireless devices.

We recognise the importance of ***autonomy*** as a key principle and another important foundation of user trust. We see it as a key requirement of any system to provide its users with the ability to specify and adjust levels of autonomy, and to reconfigure, customize or override elements of intelligent systems by making agents back off certain tasks, and allowing the user to take control. In terms of ***transparency*** and openness, it is important that potential users know how services can affect their lives in both positive and negative ways (weaknesses, limitations and potentially negative consequences). This involves making relatively *invisible* (monitoring and surveillance activities) processes more open and *visible.*

The design and development of any intelligent environment system must take into account the issues of ***equality***, ***dignity*** and inclusiveness of provision. This may involve ensuring the accessibility and affordability of devices, systems and services to primary user groups. It might also involve designing systems and devices that do not attempt to substitute for human care, but augment, support and genuinely *assist* primary users. It also extends to issues around design and usability, and ensuring social inclusiveness, by accommodating different potential levels of cognition, competence and technical ability amongst primary users. This should be done in ways that do not

threaten or undermine the dignity of primary users, for example by stigmatising those with physical or mental impairments, but reassure and support them.

# CONCLUSION

There are a number of fundamental issues that need to be considered when developing ethical frameworks for the development of intelligent environments. We explicitly identified the main ethical concerns addressed by previous work as well as highlighting the relevance of other concerns, which are important but have been overlooked so far. Whilst previous work on the ethical dimension of Intelligent Environments has been valuable, we have presented a more holistic approach that might influence the area at an engineering level and make a concrete difference in the real world by benefitting final users more directly. The issues presented are an interesting challenge for the community to explore more in depth how this ethical framework can be embedded in other software development methodologies.

# REFERENCES


Aarts, Emile (2004) Ambient Intelligence: A Multimedia Perspective, IEEE MultiMedia, v.11 n.1, p.12-19

Albrechtslund, A. 2007 House 2.0: Towards an Ethics for Surveillance in Intelligent Living and Working Environments, CEPE 2007: Seventh International Computer Ethics Conference

Augusto, J., Callaghan, V., Kameas, A., Cook, D., Satoh, I. (2013a) Intelligent Environments: a manifesto. *Human-Centric Computing and Information Sciences*, 3:12, Springer. DOI: 10.1186/2192-1962-3-12 URL: http://www.hcisjournal.com/content/3/1/12

Augusto, J., Grimstad, T., Wichert, R., Schulze, E., Braun, A. Rdevand, G.M., Ridley, V. (2013b) *Personalized Smart Environments to Increase Inclusion of People with Down's Syndrome*. Proceedings of 4th International Joint Conference on Ambient Intelligence. pp 223-228. 3rd-5th December, 2013. Dublin, Rep. of Ireland. Springer Verlag.

Augusto, J.C., McCullagh, P.J., Augusto-Walkden, J-A. (2011) Living without a safety net in an Intelligent Environment. EAI Endorsed Trans. Ambient Systems 1: e6. http://eudl.eu/doi/10.4108/trans.amsys.2011.e6

Ball, M., and Callaghan, V. (2011) "Perceptions of Autonomy: A Survey of Users' Opinions Towards Autonomy in Intelligent Environments", *Intelligent Environments* Conference, Nottingham 27-29th July 2011

Beauchamp T.L. and Childress J.F. (2001) *Principles of Biomedical Ethics*, Oxford University Press, Oxford.

Bohn, J., Coroama, V., Langheinrich, M.,Mattern, F., and Rohs, M. 2004. Living in a World of Smart Everyday Objects—Social, Economic, and Ethical Implications, Human and Ecological Risk Assessment, Vol. 10, No. 5, October

Brown, I. and Adams, A. (2007) Ethical Challenges of Ubiquitous Healthcare, *International Review of Information Ethics*, Vol. 8, No 12. pp. 53-60

Callaghan, V., Clarke, G. and Chin, J. 2009. Some socio-technical aspects of intelligent buildings and pervasive computing research. Intelligent Buildings International 01/2009; 1(1):56-74.

Chan, Marie. Campo, Eric. Estève, Daniel. Fourniols, Jean-Yves (2009) Smart homes — Current features and future perspectives, Maturitas 64 90–97

Coeckelbergh, Mark (2010) Health Care, Capabilities, and AI Assistive Technologies, *Ethical Theory Moral Practice* 13: pp. 181–190

Coughlin, J.F. D'Ambrosio, L.A. Reimer and B. Pratt, M.R. 2007 Older Adult Perceptions of Smart Home Technologies: Implications for Research, Policy & Market Innovations in Healthcare (online reference)

Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P., And Heinonen, S. 2005 Perspectives of ambient intelligence in the home environment. Telematics Informatics, 2005. 22, Elsevier, 221–238.

Ikonen, V. Kaasinen, E. and Niemelaa, M. 2009 Defining Ethical Guidelines for Ambient Intelligence Applications on a Mobile Phone. Workshops Proceedings of the 5th International Conference on Intelligent Environments, Ambient Intelligence and Smart Environments Series, Volume 4, pages 261-268. IOS Press.

Landau, R. Auslander, G. K. Werner, S. Shoval, N. and Heinik, J. 2010 Families' and Professional Caregivers' Views of Using Advanced Technology to Track People With Dementia, Qualitative Health Research 2010 20(3): pp. 409-419

Langheinrich, M., Coroamă, V., Bohn, J., Friedemann, M. (2004) Living in a Smart Environment – Implications for the Coming Ubiquitous Information Society, *Telecommunications Review*, Vol 15 (1) pp. 132-143

Nussbaum, M. C. (2006) Frontiers of justice: disability, nationality, species membership. Harvard University Press, Cambridge M.A. and London

Nixon, P. Wagealla, W. English, C. Terzis, S. 2004 Security, Privacy and Trust Issues in Smart Environments. In "Smart Environments". Cook, D. and Das, S., Eds., pp. 220-240.Wiley.

Oishi, Meeko Mitsuko K. Mitchell, Ian M. and Machiel Van der Loos, H. F. (Eds) 2010 *Design and Use of Assistive Technology: Social, Technical, Ethical, and Economic Challenges*, Springer

Perry, J., Beyer, S., & Holm, S. (2009) Assistive Technology, Telecare And People With Intellectual Disabilities: Ethical Considerations. *Journal of Medical Ethics*, 35, 81–86.

Rashidi, P. 2012 A Survey on Ambient Assisted Living Tools for Older Adults, IEEE Transactions on Information Technology in Biomedicine, vol. X, no. X

Sadri, F. (2011) Ambient Intelligence: A Survey, *ACM Computing Surveys*, No. 36, Vol 43 Issue 4

Schülke, A. , Plischke, H. and Kohls, N (2010) Ambient Assistive Technologies (AAT): socio-technology as a powerful tool for facing the inevitable sociodemographic challenges? *Philosophy, Ethics, and Humanities in Medicine*, 5:8

Sharkey, A. and Sharkey, N. (2012) Granny and the robots: Ethical issues in robot care for the elderly. *Ethics and Information Technology*, Vol 14, Issue 1, pp 27-40

Sliwa, J. and Benoist, E. (2011) Pervasive Computing - the Next Technical Revolution, *IEEE Developments in E-systems Engineering*

Van Heerde et al, (2006) Balancing smartness and privacy for ambient intelligence. Proceedings of the 1st European conference on Smart Sensing and Context (EuroSSC).

Van Hoof, J., Kort, H.S.M., Markopoulos, P., Soede, M. (2007) Ambient intelligence, ethics and privacy, *Gerontechnology*, Vol 6, no 3: pp. 155-163, published by the International Society for Gerontechnology

Van Hoof, J. Kort, H.S.M. Ruttenb, P.G.S. and Duijnstee, M.S.H. (2011) Ageing-in-place with the use of ambient intelligence technology: Perspectives of older users, *Int. Journal of Medical Informatics*, 80, pp. 310–331

Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E., & Punie, Y. (Eds) (2010) *Safeguards in a World of Ambient Intelligence.* New York: Springer