Joshua Hogue

Coach Ryan

AP English III

22 February 2016

What AmI?

He sprints downstairs from the bedroom in a panic, late after hitting the snooze button one too many times. He is running out of time. "Where are my keys?" he wonders aloud. A gentle, computerized voice rings overhead: "Your keys are on the barstool in the kitchen." The man rushes to the kitchen, grabs the keys from the barstool, devours a pre-cooked breakfast lying on the counter, and heads out to begin his day, which could have had a disastrous start. How did this man make it on time to work? What made this possible? The answer lies in a technology that could change the world as we know it forever: Ambient Intelligence.

What is Ambient Intelligence? As MIT Professor Patricia Maes puts it, Ambient Intelligence, or AmI, is the art of integrating the digital and physical reality. It is channeling information from the real world to smart devices which can process and act on the data they receive. These devices can be internal or external. Internal devices move with the user and can include cell phones, wearable technology like Google Glass, or implanted microchips that can be identified by other devices (Wolinsky). Alternatively, an example of an external device would be the tracer microchip that allowed for the man in the scenario to find his keys. Everyday objects could be given life through simple, inexpensive devices called Radio Frequency Identification or RFID chips (MIT Project Oxygen). These chips would store data from their surroundings and provide users with useful information, like an object's location or condition. AmI begins when

several of these devices are linked together and operate through a versatile, easy to use software network (Weiser, qtd. in Punie). Once the data is compiled, robots, environmental fixtures, or other devices will be able to issue responses that help people accomplish tasks and achieve their goals (Cook).

Why spend the time and money to invest in AmI? For one, humans are not perfect. As Patricia Maes explains, we have clear limits on our processing power and cognitive abilities. Ambient technologies would not only help us to overcome these limitations, but they would also help us to expedite a wide variety of tasks. These tasks can range from simple, everyday actions like unlocking doors, or more complex actions such as making transactions or proving identity. Further investment in AmI would lead to people becoming even more time-productive and aware in the future (Maes).

Of course, there are concerns about the implementation of AmI, as there are with any new technology. People have been concerned since the very beginning of its development about hackers, practices like data mining, and similar exploitations of privacy (Wright). While these practices are still alive and well today, AmI will provide new, diverse, and more widespread mediums to act and prey on privacy. Among other concerns are the enforceability of laws involving public and private AmI spaces and the theft of intellectual property. AmI needs to develop further and address these concerns before it can be realized as a worldwide or public system, but that fact alone should not discredit its current applications, potential, or usefulness.

Ambient Intelligence should not be written off as dystopian, invasive technology. With the proper safeguards and tools, it has incredible applications that could revolutionize our private, professional, and public lives.

Civic applications for AmI are plentiful. Whether for use in airports, government facilities, or just crowded spaces, sensors could be integrated to help detect threats earlier and save lives. The United States Department of Defense has already begun to display interest in the use of AmI networks to strengthen national defenses (Wolinsky). In addition, sensor networks in public buildings could provide information concerning structural integrity, preventing unnecessary injuries and deaths through early-warning disaster systems (Cook). By monitoring traffic conditions and calculating speeds, AmI systems could be used as a public service to direct traffic safely and efficiently across multiple road routes (Wright). In addition, any accidents that would happen would be reported faster, cutting response times. There are dozens of other ideas in circulation merely for civic use, let alone private use.

Healthcare could also benefit greatly from AmI tech. RFID chips could be used to easily monitor the elderly, the mentally unstable, the chronically ill, and the incapacitated. In 2006, William Koretsky, a New Jersey police officer, was recovered unconscious from a serious car accident (Wolinsky). He was unable to communicate with his caretakers and nothing recovered from the accident revealed any of his medical conditions. But upon scanning him in the ER, nurses were able to find an RFID chip implanted in his arm which gave them access to his medical records. They found that he was a diabetic. The caretakers from that point onward carefully monitored Koretsky's blood sugar levels as they nursed him back to health. That RFID chip and the data it provided to caretakers may have saved Koretsky's life from a faulty treatment or a spike in blood sugar. In a similar way, these chips could be used to save the lives of people under similar circumstances by reporting medical conditions or marking the locations of trapped survivors.

The professional environment has uses for AmI as well, as demonstrated by an experimental project called "Verichip" in Florida. Verichip allowed participating business executives to gain quicker access to areas requiring higher security clearance without expensive biometric identification systems (Foster). In addition, employees participating in the Verichip project gained a personalized credit card system which allowed them to make transactions with local companies. New economic systems arising from Ambient Intelligence have already been used around the world to prevent the theft of expensive prescription medicines and other merchandise (Wolinksy). With these economic systems in place, businesses and corporations could gain an enhanced level of security at the minimal cost of a few microchips.

One of the barriers to the implementation of AmI technology over the years has been the development of the creative, efficient technology required to implement it. Previously, small enough processors, sensors, and embedded networks were out of reach due to costs of production. But now, as the Verichip program demonstrated, the technology exists now and can be implemented effectively (Foster). “Intelligent Spaces” with integrated AmI technology have been in development since 2007 in Stanford’s AIR lab and MIT’s Project Oxygen, both of which aim to make technology “as natural as the air we breathe”. The Ambient Intelligence Research (AIR) lab is developing smart, gesture controlled environments using smart cameras (Aghajan). These environments could be used to make buildings more energy efficient and aware of their occupants, saving homes and businesses thousands of dollars a year in energy usage. Project Oxygen, on the other hand, has been focused on software networking from both mobile and stationary sensors, and secure access of data (MIT Project Oxygen). By combining both smart surveillance and secure networking technologies, AmI systems will be well within our reach.

It is also possible to build safeguards into these AmI systems in order to address privacy concerns, vulnerabilities, and user error. First, it would be necessary to divide a user's roles into three main categories: a private mode, a professional mode, and a public mode and three levels of control for each (Wright). Each of the modes would have varying levels of security and access to different information. These environmental adaptations will allow data and data collection of a user to be airtight at all times. For example, in a public setting security would be heightened to protect a user's personal information, such as their location. But in a professional setting, employers need to access this information in order to monitor their employees, ensuring that they are on task during work hours.

When AmI needs to make its own decisions, three modes of control will be presented: High (the system makes its own decisions), Medium (the system asks the user for advice on a decision), and Low (the system only does what the user tells it to do) (Wright). The varying levels of control that a user gives to AmI will depend on the decisions the AmI is forced to make. For a major decision, such as broadcasting data to others, the user needs to feel in control of the situation in order to feel comfortable. But for a minor decision, like deciding to turn off lights in an empty room, presenting a decision to the user would quickly become tedious and repetitive, like a toddler that asks too many questions. But by changing a user's control and security based on their environment, an AmI system could efficiently run in any type of environment, not just the home or the office.

Creative programs and business models for AmI provide ways to keep both customer and provider security. Some of the suggested ideas include the use of pseudonyms, cell phone-esque service contracts, software validation programs such as the TRUST program being developed at

Berkeley, and "cooperative file systems". (Wright, Project Oxygen) These cooperative systems would decentralize data collection, greatly hindering a hacker's efficiency and likelihood of success. All of these programs would provide an additional cushion of security between the user, their data, and people who access their data.

Opponents of Ambient Intelligence applications include privacy advocates who claim that the technology will lead to rampant breaches of privacy both inside and outside the home. The very walls would listen to our conversations, watch our movements and welcome unwanted spectators, such as the government. But in reality, Ambient Intelligence would not change our current state of privacy in the United States. The NSA already has lawful access to almost any digital content we publish or view thanks to programs like PRISM and Boundless Informant, which were exposed by Edward Snowden (Handley). Phone records can now be tapped without a search warrant thanks to the verdict of the Smith v. Maryland SCOTUS case (Slobogin). But the government does not have the power to monitor every second of our every day; it would take up too much time and manpower. The conditions for an Ambient Intelligent world would be almost identical. We already have the framework of an Ambient Intelligent world at our fingertips with smart phones and other devices. In short, an AmI environment should not make us feel any more paranoid or violated than we are now. If all goes well, national security data collection should still be limited to a bare minimum, like it is now. As Professor Richard Lempert of the University of Michigan stated, "privacy remains a cherished human value" (qtd. in Handley).

A more extreme postulation of the Ambient Intelligence debate goes beyond surveillance to control. Some fear that the government will use Ambient Intelligence, which would guide our everyday lives, to manipulate our thoughts and actions like ants (Verbeek). Ambient Intelligence

would never progress to that stage. Social acceptance and trust in technology is just as important as the development of the technology (Punie). As we saw with Google Glass, if consumers feel uncomfortable with AmI interfaces, then they simply will not use them. If Ambient Intelligence started to progress in that direction, individuals will always have the option of disconnecting themselves from the software.

As a diversely applicable and hugely beneficial technology, Ambient Intelligence has the power to transform the world several times over. But before this can happen, as a society, we need to be ready to accept its terms and conditions. But the leaps that people have made in the past to cell phones, portable computers, and other devices prove that this jump to AmI be pursued.

Works Cited

Aghajan, Hamid, (Lab Director). "JAISE - Forum." *A I R Lab*. Stanford University, 2007. Web. 14 Feb. 2016

Cook, Diane J., Juan C. Augusto, and Vikramaditya R. Jakkula. "Ambient Intelligence: Technologies, Applications, and Opportunities." *Wsu.edu*. Washington State University, 3 Oct. 2007. Web. 14 Feb. 2016.

Foster, Kenneth R., and Jan Jaeger. "The Murky Ethics of Implanted Chips."*Upenn.edu*. University of Pennsylvania, Mar. 2007. Web. 9 Feb. 2016.

Handley, John. "PRISM AND BOUNDLESS INFORMANT: IS NSA SURVEILLANCE A THREAT?"*American Diplomacy* (2013). *Opposing Viewpoints in Context*. 17 Jul. 2013. Web. 14 Feb. 2016.

Maes, Patricia. "Lecture Notes." *MIT Open CourseWare*. Massachusetts Institute of Technology, 2005. Web. 15 Feb. 2016.

"MIT Project Oxygen." *MIT Project Oxygen*. Massachusetts Institute of Technology, 2007. Web. 11 Feb. 2016.

Punie, Yves. "A Social and Technological View of Ambient Intelligence in Everyday Life: What Bends the Trend?" Institute for Prospective Technological Studies Directorate General Joint Research Centre European Commission, 2003. Web. 10 Feb. 2016.

Slobogin, Christopher. *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*. Chicago: U of Chicago, 2007. Print.

Verbeek, Peter-Paul. "Ambient Intelligence and Persuasive Technology: The Blurring Boundaries Between Human and Technology." *Nanoethics*. Springer Netherlands, 2009. Web. 17 Feb. 2016.

Wolinsky, Howard. "Tagging Products and People. Despite Much Controversy, Radiofrequency Identification Chips Have Great Potential in Healthcare." *EMBO Reports*. U.S. National Library of Medicine, 7 Oct. 2006. Web. 09 Feb. 2016.

Wright, David, Elena Vildjiounaite, Ioannis Maghiros, Michael Friedewald, Michiel Verlinden, Petteri Alahuhta, Sabine Delaitre, Serge Gutwirth, Wim Schreurs, and Yves Punie. "Safeguards in a World of Ambient Intelligence (SWAMI)." *Ist.psu.edu*. Fraunhofer Institute for Systems and Innovation Research, Jan. 2006. Web. 10 Feb. 2016.