Ubiquitous Computing: The Technology for Boundless Surveillance

Edem Williams (Corresponding author) and Bassey Eyo
Dept. of Maths/Stats and Computer Science
University of Calabar, Calabar, Nigeria
E-mail: edemwilliam@yahoo.com

ABSTRACT
Mainstream and advanced surveillance technologies are limited in terms of their reach in monitoring and tracking people and objects despite the dearth of spatial boundaries. This limitation could possibly be eliminated with the advent of ubiquitous computing. The application of ubiquitous computing in surveillance is such as could take advantage of spatial boundlessness to effect a real time boundless surveillance. This paper suggests that the reach of ubiquitous computing in surveillance cannot be hindered except humans step in to define its delimiters of operation.

Author Keywords
Ubiquitous computing, technology, surveillance, mainstream,

INTRODUCTION
The term 'Ubiquitous Computing' (Ubicomp) [23] was coined by Mark Weiser in 1991 as he envisaged a world where computers would 'weave themselves into the fabric of everyday life until they are indistinguishable from it' [23 p.1]. Weiser defined ubiquitous computing as 'the method of enhancing computer use by making many computers available throughout the physical environment making them effectively invisible' [24 p.1]. Weiser's vision propelled a paradigm shift in the relationship between computing and society [22] with enabling technologies for its application embedded everywhere (in objects, people, and places) [9]. areas of application. According to Genevieve and Dourish, '...Ubicomp technologies prove also to be Ubicomp provide possibilities of a wide range of sites of social engagements, generational conflict, domestic regulation, religious practices, state *surveillance*, civic protest, romantic encounters, office politics, artistic expression, and more' [3 p.141]. But I believe that the above list of areas can be categorized into two areas; all the areas listed except surveillance can be categorized as social. Hence, I would suggest we have surveillance and social applications of ubicomp.

Anne Uteck [22] suggest that the idea of ubicomp as a tool for surveillance is intriguing because there are already in existence technologies that extends the ability to locate and track people and things in the real world any where, anytime, accurately, continuously, and in real time . Despite this view, I believe that the advancement in technologies that aid mankind to achieve a specific goal cannot grind to a halt as a result of the existence of mundane technologies meant for that same purpose; new technologies tend to expose the limitations of old ones.

This paper does not focus on 'the world of Sal' [9] as contained in Mark Weiser's paper – "The Computer for the 21st Century," where everything works according to Sal's wish, I will be focusing on a real world applicability of ubicomp – surveillance, and possibilities for the convergence of existing surveillance technologies to achieve this.

An insight into the current usage of existing surveillance technologies is given below, followed by their limitations, and a review of how the integration of these surveillance technologies can be intertwined with ubiquitous computing surveillance potentials and operational challenges of ubicomp as a tool for boundless surveillance.

TECHNOLOGICAL DIMENSIONS TO SURVEILLANCE

The progression from mainstream surveillance technologies such as credit and affinity cards, closed circuits television (CCTV), red light cameras, biometric systems, tracking software, thermal imaging, etc to advanced surveillance technologies such as Radio Frequency Identification (RFID), Global Positioning System (GPS) and advanced wireless technology set the stage for seamless, real-time surveillance [22]. Martin Dodge et al in their work 'No longer lost in the crowd' claim that these advanced surveillance technologies provide the capability of directed surveillance throughout the environment with the goal of monitoring people everywhere at all times [7].

The mainstream technologies as listed above have their own well defined advantages for surveillance, but my focus is on the three aforementioned advanced surveillance technologies and their area of applications in the larger society.

Radio Frequency Identification (RFID)

According to Garfinkel and Rosenberg [8], RFID is a micro-chip technology which uses radio signals to identify objects that are embedded with RFID transmitting tags. Because of their miniaturized status it is easy to conceal them in other items. For instance, in order to study the behaviour of live ants, researchers at Bristol University earlier this year (2009) successfully glued RFID micro-transponders to these ants [10].

RFID is being deployed in e-passports production by the United States (US). The same information that is printed within the passport is stored in the chip inlays (produced by Smartrac), implying that the holder's travel history will be recorded in the chip [11]. In order to control access to the RFID reader, the US State Department developed a Basic Access Control (BAC) to enable the encryption of communications between the reader and the chip [17].

Uteck [22] claim that Public Libraries are seeking to engage RFID tags in tracking their books to communicate the identity of a borrower. RFID tags have been used already to tag some adults and juveniles to ensure compliance with bail conditions in the United Kingdom [15].

It is also being used in transportation and logistics, as Emirates Airline in Feb, 2008 test ran RFID baggage tracing at London and Dubai Airports [29]. Also, in the railroad sector, RFIDs are being deployed to indicate the origin and destination of the goods being carried by the cargo train [20]. In Canada, RFIDs are used in a pay-as-you-go system of highway and bridge tolls [22]. As technology becomes cheaper and advanced by the day, RFIDs may be deployed in almost every sector of human endeavour for the purpose of surveillance.

Global Positioning System (GPS)

Global Positioning System (GPS) is a satellite navigation system that uses radio transmissions to determine the exact location of people and machinery whether they are on land, sea, airborne, regardless of the weather conditions, anywhere in the world [14].

GPS is also a tagged surveillance system which requires that components are attached to the dynamic entity (GPS receiver on vehicles, persons, etc) and the static entity (satellite) also. The dynamic entity's location is determined by the measurement of its environmental property (via radio wave) by satellites that are placed in the environment [25].

Uteck [22] posits that GPS has progressed from traditional military usage to a multi-satellite network aiding real time surveillance in non military, civilian and consumer applications. The military application of GPS is vast. For example it is being used to aid ground troops in the location of targets in the dark or in unfamiliar terrain. Also, it assists commanders in the co-ordination of troop movement and supplies [19].

Some civilian applications have also gained from GPS deployment. Mark Monmonier [14] reports that it is being used for the purpose of crash investigation and traffic system performance analysis [26]. In addition, it has become an accepted tracking device in vehicles [21] and is used for monitoring employees [16] and tracking prisoners that are on parole [18].

Advanced Wireless Technologies

Collin Bennett and Lori Crowe [4] view the emergence of Advanced Wireless Technologies such as Wireless Fidelity (Wi-fi) as a supplement for the communication demands of the world. Wi-fi permits devices that are equipped with Wi-fi based wireless network cards to access the internet from its base station. Wi-fi technology is attaining increased patronage with its nodes (also known as hotspot) taking up presence in shopping malls, airports, hotels, public libraries, educational institutions, etc [22].

The potential for observing and tracking physical movement of entities connected to the Wi-fi network is certain as it is claimed by Uteck [22] that there is a plan by wireless Internet Service Providers to create mesh networks of hotspots. Organizations are also deploying Bluetooth-based surveillance systems [28] that uses wireless technology for the purpose of interconnecting various bluetooth wireless enabled devices such as Personal Device Assistants (PDA), laptops, mobile phones, etc [22].

SURVEILLANCE LIMITATIONS OF EXISTING TECHNOLOGIES

RFID tagged objects can be tracked by systems that are designed to reconstruct the objects' route. The RFID chip has a read-write memory with capabilities to store location details from system transmitters. The system requires the tagged object be positioned along the circulation network [22]. This is a set back for RFID technology because if the object goes out of its sphere of contact, then it is not going to be possible to track the object.

On the other hand, GPS' tracking capability is continuous, especially when connected to a mobile system in real time but signal corruption in certain areas can affect its tracking capability [22]. For example in vehicle GPS receivers, metallic framing of windshields [27], such as tinting films for car windows can degrade the reception just inside the car [26].

Cerruti et al [6] claim that the weather condition in space can also corrupt GPS signal by direct interference with solar radio burst noise in the same frequency band while Aarons et al. [2] posit that the diffusion of the GPS radio signal in ionospheric irregularities brings about an interference referred to as scintillation. Scintillation takes place more in tropical latitudes

when at night time than in high latitudes or mid-latitudes where magnetic storms can lead to scintillation [13].

UBIQUITOUS COMPUTING AND SURVEILLANCE

Keeping track of people on a daily basis is as old as time itself, as was obtainable in village settlements where peer groups kept watch over their subject of interest, while vigilantes kept watch over the village, and if any negative or suspicious behaviour was observed, the society at large would be notified [12].

These mundane and manual surveillance methods have been replaced by machines which have virtually become watchers over mankind as could be seen above in the listings of the mainstream surveillance technologies and review of existing advanced surveillance technologies, but there is more.

Mark Weiser's vision of a world in which computation would be physically, socially and procedurally embedded in our daily activities might not have taken the shape he envisaged, but the presence of surveillance technologies such as the RFIDs, GPSs, etc have a semblance to the machines that Weiser imagined would occupy our world today [1].

The aim and objective of ubicomp is to avail mankind of virtual machine services [5]. Ubiquitous computing applications would have more powerful personal information collation and distribution [3] than existing technologies; it will extend the capabilities of existing surveillance technologies.

INTEGRATION OF SURVEILLANCE TECHNOLOGIES

According to Genevieve and Dourish, Ubiquitous computing '...encompasses a wide range of disparate technological areas, brought together by a common vision' [3 p.1]. The individual technologies as discussed earlier have a common *vision* which is *surveillance,* and bringing them together under the same umbrella would serve the purpose of enhanced surveillance.

The convergence of these surveillance technologies could result in a powerful and complementary surveillance system which can assist organizations, government, etc in tracking and instantaneously determining the location of individuals and objects of interest whether mobile or static[22].

The complementary roles of these technologies stems from their individual limitations. These limitations are more or less the boundary points of their surveillance capabilities. These limitations can be eliminated with the amalgamation of these three technologies, because Radio Frequency Identification extends Global Positioning Systems tracking capabilities while advanced wireless technology takes care of the real-time requirement of the group [48].

The geo-spatial coverage of GPS and RFID's individual tagging of objects when integrated takes surveillance to a ubiquitous height, because ubiquitous computing surveillance applications would be everywhere [9], it will serve as the all-seeing-eye; what I would refer to as surveillance without borders.

OPERATIONAL CHALLENGES

The notion of boundlessness of ubiquitous computing brings into bear the issue of privacy. Anne Uteck posits that 'the seamless integration of these technologies into spaces and places of our everyday lives, more directly and more pervasively, compromises physical and social

boundaries in private and public spheres' [22 p.84]. This is unarguably true because the spatial coverage of ubiquitous computing as a tool for surveillance would provide unhindered access to the *monitored* for the *monitor* (governments, organisations, etc).

Also, Mark Dodge suggest that this technology is such '...that identifies uniquely you and has the potential to actively 'leak' your positional data (at varying resolutions) to a control network and thus to third parties' [7 p.16]. I believe that these *third parties* may not necessarily be the wrong people gaining access to one's positional data, but also the *monitor* gathering information about the *monitored* which fall outside the purpose or scope of the surveillance could be considered as *third parties.*

The above issues call for the definition of operational boundaries for ubicomp as a tool for surveillance. A statement made by Prof. Gary T. Marx as cited in Mark Langheinrich's paper *Privacy invasions in Ubiquitous Computing* says that "Central to our acceptance or sense of outrage with respect to surveillance ... are the implications for crossing personal borders" [12 p.4]. This statement is a concession to the boundlessness of ubiquitous computing surveillance technologies and a clarion call for legal framework for operational boundaries for these technologies.

Prof. Marx went further to categorise the operational boundaries as natural, social, spatial or temporal, and transitional effect borders [12]. Whether these boundary definitions by Prof. Marx or various legal activists, groups, etc would be considered is left to be seen, as this must have to be ratified by the judiciary of independent nations that have these technologies operating therein.

CONCLUSIONS

The idea of a boundless technology for surveillance may provoke legal fireworks, but for governments, organizations and even individuals that will benefit from such a technology, this is a step in the right direction.

Indeed, the mainstream and advanced surveillance technologies that are already in use today are veils over the real masquerade – *ubiquitous computing*. With the existence of these technologies, Mark Weiser's vision of the future is partially here.

Whichever name they are called, whether RFID, GPS, etc, they all possess characteristics of ubiquity and boundlessness. It is left for regulators to define their borders of coverage in terms of privacy laws that are directed at their scope of operation.

REFERENCES

[1] Abowd, G. and Mydnatt, E. *Charting past, present and future research in Ubiquitous Computing*. ACM Transactions on Computer-Human Interaction 7 (1), 2000 pp. 29-58

[2] Aarons, J., and Basu, S. *Ionospheric Amplitude and Phase Fluctuations at the GPS Frequencies.* Proceedings of ION GPS v2, 1994. pp 1569-1578

[3] Bell, G. and Dourish, P. *Yesterday's Tomorrows: Notes on Ubiquitous Computing Dominant Vision.* Personal Ubiquitous Computing 2 (2) p141 2007. Available from: http://portal.acm.org/citation.cfm?id=1229069 [accessed 16 November 2010]

[4] Benneth, C. and Crowe, L. *Location-based Services and Surveillance of Mobility: An Analysis of Privacy Risk in Canada.* A Report to the office of the Privacy Commissioner of

Canada. 2005. Available from: http://web.uvic.ca/polisci/bennett/pdf/lbsfinal.pdf [accessed 11 November 2010]

[5] Beresford, A. *Locational Privacy in Ubiquitous Computing.* Technical Report No. 612, University of Cambridge Computer Laboratory. UCAM-CL-TR-612 ISSN 1476-2986 2005

[6] Cerruti, A. Kintner, P., Gary D., Manmucci, A, Meyer, R., Doherty H., and Coster, A. *Effect of intense December 2006 Solar Radio Bursts on GPS Receivers.* Space Weather. 2007. doi: 10.1029/2007SW000375

[7] Dodge, M., Batty, M., and Kitchin, R. *No Longer Lost in the Crowd: Prospects of Continuous Geosurveillance.* Association of American Geographers Conference 2004. Available from: http://www.casa.ucl.ac.uk/martin/aag_geosurveillance.pdf [accessed 16 November 2010]

[8] Garfinkel, S. and Rosenberg, B. (eds). *RFID: Application, Security and Privacy.* New Jersey, Pearson Educational Inc. 2005 pp 3-36

[9] Greenfield, A. *Everyware: The Dawning Age of Ubiquitous Computing.* Berkerley, CA New Riders. 2006

[10] Home Search Habit of Ants uncovered. Available from: http://news.bbc.co.uk/1/hi/england/bristol/8011998.stm [accessed 16 November 2010]

[11] Inlays from SMARTRAC. 2006. Available from: http://www.contactlessnews.com/2006/11/30/contactless-inlays-from-smartrac-ordered-for-us-epassport-project. [accessed November 03 2010]

[12] Langheinrich, M. *Privacy Invasions in Ubiquitous Computing.* 2002. Available from: http://www.vs.inf.ethz.ch/publ/papers/langhein2002-ucpws.pdf [accessed November 03 2010]

[13] Ledvina, B., Makela, J. and Kintner, P. *First observations of intensed GPS L1 Amplitude Scintillations at Mid Latitude.* Geophy.Res.Lett., 29 (14), 1659, Doi:10.1029/2002GL01, 2002.

[14] Monmonier, M. *Spying with Maps: Surveillance Technologies and the Future.* Chicago, The University of Chicago Press. 2002

[15] National Probation Service Bulletin. *Electronic Monitoring 6*. 2006. Available from: http://www.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes

[16] Peterson, A. *Understanding Surveillance Technologies: Spy Devices, Privacy, History and Applications.* (2nd ed) Boca Raton, Taylor and Francis. 2007 p337

[17] Prince, P. *United States sets date for E-passports*. 2006. Available from: http://rfidjournal.com/article/articleview/1951/1/132 [accessed 16 November 2010]

[18] Pro Tech. Available from: http://www.ptm.com [accessed 03 November 2010]

[19] Sinha, V.. *Commanders and Soldiers' GPS Receivers*. 2003. Available from: http://www.gcn.com/print/22 20/22893-1.html

[20] Soft trail by AEI Technology. *Softrail*. 2008. Available from: http://www.aeitag.com/aeirfid.html [accessed 03 November 2010]

[21] Solutions into Motion. Available from: http://www.trackem.com [accessed 03 November 2010]

[22] Uteck, A. *Ubiquitous Computing and Spatial Privacy*. In: Ian Kerr, Valerie Steeves, Carole Lucock (eds). *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. 2009 pp 83-101. Available from: http://www.idtrail.org/files/ID Trail Book/9780195372472.kerr_05.pdf [accessed 17 November 2010]

[23] Weiser, M. *The Computer for the 21st Century*. Scientific American 265 (3). 1991 p1. Available from:http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html [accessed 30 October 2010]

[24] Weiser, M. "*Hot Topics: Ubiquitous Computing*" *IEEE Computer*.1993 p1. Available from:http://www.ubiq.com/hypertext/weiser/UbiCompHotTopics.html. [accessed 03 November 2009]

[25] Welch, G. and Foxlin, E. *Motion Tracking: No Silver Bullet, but a respectable Arsenal.* IEEE Computer Graphics and Applications 22 (6) 2002. Available from: http://ieeexplore.ieee.org/iel5/38/22427/01046626.pdf [accessed 03 November 2010]

[26] Window Films. 3M Automotive Films. Available from: http://solutions.3m.com/wps/portal/3M/enUS/WF/3MWindowFilms/products/productCatalog/?PC [accessed 16 November 2010]

[27] Windshield. *I-Pass Mounting for vehicles with special Windshield features.* Available from: http://www.illinoistollway.com/pls/portal/docs/PAGE/TW CONTENT REPOSITOR Y/TW CR IPASS/LPT.SPECIALWINDSHIELD.pdf [accessed 16 November 2010]

[28] Wireless Technologies and Blutooth. Intel Technology Journal 4 n.2 2002. Available from: http://intel.com/technology/itj/archive/2000.htm [accessed November 14 2010]

[29] World Airline News. *BAA and Emirates test new baggage tagging Technology*. 2008. Available from: http://jetvine.blogspot.com/2008/02/baa-and-emirates-test-new-baggage.html [accessed 17 November 2010]