CSC3723 – Reflective Blog

What is Security and Privacy?

Privacy and security before Ubicomp technology was relatively simple to define and regulate. This is because times were simpler, there were just significantly less ways that people can collect data about other people. Bohn (2005) describes what personal privacy rules are and how they should be interpreted.[1] The four main points are, natural borders (such as walls, clothing, darkness), social borders (social groups, such as family members), spatial or temporal borders (such as undisclosed parts of someone’s life) and borders due to ephemeral or transitory effects (spontaneous actions will soon be forgotten). These rules are upheld in society to protect and regulate the public and people’s personal lives. Privacy now must deal with ever growing technology to protect people’s data and personal information. As people’s data is stored from applications and accounts created by companies, they have a responsibility to you as a user to hold the information safe.

Here is a video on data protection and privacy:

<https://www.youtube.com/watch?v=6vNxslcf9AE>

Security is the act of protecting people. This can be done by governing bodies or legislation which is in place to make sure people play by the rules. Here we are talking about the security of people private and confidential information. This can range from devices that record sound to monitoring your location every step you take. As technology is changing and devolving so rapidly, laws and rules cannot be applied quick enough and this is the main worry of people and their privacy. A form of security which is in place to protect people’s information online is The Data Protection Act. The Data Protection Act of 2018 has been put in place as a means of controlling what a companies or businesses can do with your personal information.[2] They regulate over such disputes which regard the use of the information given to them by the public. They follow the “Data Protection Principles” which are a strict set of rules that companies must abide by to protect people’s data.

How does new technology like activity recognition bring new issues?

There has been great interest since the turn of the century about Ubicomp and how it can integrate with our lives to make them easier and more cooperative with technology. Mark Weiser’s calm computing methodology envisions a state where people just complete tasks instead of computing.[3] For example, instead of writing a shopping list down, just talking to a smart speaker i.e. Alexa to make a note of it for you doesn’t require any computing at all. This demonstrates that technology and devices can do much more than ever imagined ten years ago and are starting to populate people’s homes and lives in almost a flash. However, these kinds of technologies are entering private spaces and can record our daily lives. Security measures should be in place but the problem with this is that the government can’t keep up with the ever-growing advances in Ubicomp. This leaves users in a vulnerable gap where they don’t have security and protecting their privacy is much harder to do. Ubicomp advances made in distinct aspects of computing, namely reachability, pervasiveness, and autonomy have made pre-existing security measures almost obsolete.[4] An example of this is activity recognition.

### Activity recognition is the ability for devices and wearables to be able to recognise and predict patterns in data from built in sensors. They are now present in everyday life weather you realise it or not thanks to smart phones and fitness trackers such as Fitbit. These devices know when a user is walking, in a car or even washing themselves. If this kind of information is stored and used without our knowledge, it would be a massive breach of security and privacy. Companies know some data is not needed and classification of data mining is essential for companies to extract and use the right data for pattern recognition. The way that this is possible is data pre-processing and activity profiling, where data sets have been made to profile an activity. Event records must be labelled first to supervise the learning process of activity recognition to ensure data is only recorded when needed to.[5]

### Image result for activity recognition

### <https://www.sciencedirect.com/science/article/pii/S016786551830045X>

### Another issue that we have discovered is the need for security with surveillance systems. These straddle the line of protecting people and invading people privacy. Security and surveillance systems have used visual processing approaches extensively to track human behaviours in public environments.[6] This is so that they can monitor and predict people behaviour by just watching them. This is called deep learning and is being used as we speak. We have been used to a hyper monitored environment seeing as the UK has the most surveillance then any other country. Coupled with the fact that we have loose laws on data protection and privacy, this could lead to a “surveillance society” and would invade the public privacy. [7]

### Image result for activity recognition and surveillance

### <https://medium.com/nanonets/how-to-automate-surveillance-easily-with-deep-learning-4eb4fa0cd68d>

How will it affect healthcare in a future ubicomp society?

in

darkness, facial expression (a natural border protecting the true feelings of a

person)

• Social Borders: expectations with regard to conﬁdentiality in certain social

groups, such as family members, doctors and lawyers, for example, the ex-

324 Vildjiounaite, Rantakokko, Alahuhta, Ahonen, Wright, & Friedewald

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission

of IGI Global is prohibited.

pectation that your colleagues will not read personal fax messages addressed

to you

• Spatial or Temporal Borders: expectations by people that parts of their

lives can exist in isolation from other parts, both temporally and spatially, for

example, a previous wild adolescent phase should not have a lasting inﬂuence

on the current life of a father of four, or a party with friends should not affect

relations with colleagues

• Borders due to Ephemeral or Transitory Effects: expectations that certain

action or spontaneous utterances will soon be forgotten or simply unnoticed

because of limitations on people’s attention and memor

Healthcare is always a big testing ground when it comes to new technology to help discover ways that we can care and monitor for people more effectively. According to the World Health Organization, the number of people in the age 60 years or older will increase from 900 million to 2 billion between 2015 and 2050[8]. This means there is going be a big spending increase to be able to keep up with growth in need of care. Furthermore, as the number of nurses and doctors will not be able to increase with this growth, we need to look somewhere else to help pick up the inventible slack. Ubicomp technology has the power to do this, with systems that will be able to work in tandem with healthcare professionals to help regulate and predict patients needs. However, as we have talked about privacy above, it could be sacrificed in order to do this. An example of this is how people’s private health records such details on sexually transmitted diseases have already been abused.[9] This is an example of profile abuse where organisations have explicit access to detailed personal information. At the moment physical control is the defence for privacy. This means that if a patient is having their heart rate taken in a hospital, the data from the heart rate monitor can only be seen by the care givers. If this data is uploaded straight to a database, remote use of this data is almost assured and who can see this information is not clear to the patient. Privacy is then not given to the patient with no way for them to be able to challenge or even realise what happens with the data.

There are also body sensors which can track a user’s vitals when outside of hospitals. Body-sensor-based 24-7 monitoring will enable remote diagnosis without the patient having to visit a hospital.[10] This can create a “life log” of sorts. If such data was given to companies such an insurance and drug related third parties, the possibility of abuse is great. Incentives could also be enabled where if heath data is disclosed to companies and even your place of work, you would be entitled to discounts and shortlisted for promotions. This sounds exiting until you realise that the reason it would be done is to monitor and exploit the data provided for their gain. This diminishes common standards of privacy and security of people explicit information.



<https://healthitsecurity.com/news/patient-privacy-impact-of-technology-worries-healthcare-leaders>

To conclude privacy and security with Ubicomp technologies needs better regulation of how data is stored and used to give the public a clearer view of where and what happens with it. Laws cannot be made quick enough and become obsolete when new uses are found. Therefore, a set of commandments is maybe a better way to tackle present and future privacy concerns as they will be more general and expansive when regarding data mining. This would allow authorities to initiate better security for people and a more transparent information of the use of people’s data.

## **References**

[4] Cs.dartmouth.edu. (2019). *Activity Recognition –*. [online] Available at: https://www.cs.dartmouth.edu/~campbell/cs65/lecture22/lecture22\_2018.html [Accessed 13 Dec. 2019].

[3] Cyborganthropology.com. (2019). *Calm Computing - Cyborg Anthropology*. [online] Available at: http://cyborganthropology.com/Calm\_Computing [Accessed 13 Dec. 2019].

[2] GOV.UK. (2019). *Data protection*. [online] Available at: https://www.gov.uk/data-protection [Accessed 13 Dec. 2019].

[10] Kim, J. (2019). *Towards a Security Policy for Ubiquitous Healthcare Systems (Position Paper)*. [online] Cl.cam.ac.uk. Available at: https://www.cl.cam.ac.uk/~fms27/papers/2006-KimBerSta-healthcare.pdf [Accessed 13 Dec. 2019].

[9] Little, L. (2019). *Ubiquitous Healthcare: Do we want it?*. [online] Bcs.org. Available at: https://www.bcs.org/upload/pdf/ewic\_hc08\_v2\_paper13.pdf [Accessed 13 Dec. 2019].

[5] Muller, G. (2019). *Security in UbiComp: Protection through Commandments*. [online] Pdfs.semanticscholar.org. Available at: https://pdfs.semanticscholar.org/4892/dc9ca42a34f3d763d62e59bc4f442612769b.pdf [Accessed 13 Dec. 2019].

[7] News.bbc.co.uk. (2019). *BBC NEWS | UK | Britain is 'surveillance society'*. [online] Available at: http://news.bbc.co.uk/1/hi/uk/6108496.stm [Accessed 13 Dec. 2019].

[6] SAGE Journals. (2019). *A review on applications of activity recognition systems with regard to performance and evaluation - Suneth Ranasinghe, Fadi Al Machot, Heinrich C Mayr, 2016*. [online] Available at: https://journals.sagepub.com/doi/full/10.1177/1550147716665520 [Accessed 13 Dec. 2019].

[1] Vildjiounaite, E. (2019). *Privacy Threats in Emerging Ubicomp Applications: Analysis and Safeguarding*. [online] Available at: https://www.researchgate.net/publication/258893387\_Privacy\_Threats\_in\_Emerging\_Ubicomp\_Applications\_Analysis\_and\_Safeguarding [Accessed 13 Dec. 2019].

[8] Who.int. (2019). *WHO | 10 facts on ageing and the life course*. [online] Available at: https://www.who.int/features/factfiles/ageing/ageing\_facts/en/ [Accessed 13 Dec. 2019].