According to National Instruments, 50 billion devices will wirelessly be connected to the Internet in the next four years, a fivefold increase from today's 10 billion devices (2015). As pervasive computing increases, the control of privacy and trust become greatly more complicated (Satyanarayanan, 2001). Widespread adaption to the Internet of Things (IoT) could contribute invaluably to our economy, but with everyday objects becoming security risks, the Internet of Things provides opportunities for enemies of the United States and criminals (National Intelligence Council, 2008).

Technical Topic (*Smart House*):

The Internet of Things is a future where intelligence flows through the universe of physical objects (Wasik, 2013). The ability to handle data to create a user customized experience provides developers who can meet this demand of secure and reliable solutions with a great opportunity (Wind River, 2014). Under the guidance of Professor Harry Powell, Sri Kodakalla, Alex Park, Brooke Rutherford, Mike Wang, and I will look beyond the black box of the Internet of Things. Our capstone project is to use a Leap Motion Sensor to communicate with a myRIO in order to control various household devices, such as lights, fans, and blinds (Hanson, 2015).

The Leap Motion Sensor takes in an input of hand gestures. Based off the hand gestures, a signal will wirelessly be sent to the myRIO, which will in turn control the circuits of the lights and like devices. This project, named Smart House, is semester long simplification of the Internet of Things, in which embedded systems are used to facilitate decisions based off human interaction and the communications between devices. In building a device that will serve as one of the billions connected to the wireless Internet, my team will be able to understand more about the security of the black box systems that will vastly be trusted in the future. As engineers in an emerging field, this hands-on work provides the opportunity to gain knowledge of what security and social aspects need to be considered, especially if we ever find ourselves working in a related industry.

STS Topic (*Will Privacy End in the Future?*):

For my STS topic, I will examine the security issues of the Internet of Things to better understand how pervasive computing may alter societies value on privacy. With a user's movements, behavior patterns and habits being recorded and shared amongst devices, it is likely privacy and trust will be enduring problem for the Internet of Things. The outcome of a complex system with an enormous amount of connections between autonomous actors is a chaotic environment where privacy exploitations, by companies and the government, are of major concern (Tucker, 2014). There has been controversy over related exploitations for as long as technology has been around, from the NSA spying on United States citizens to the New York Times' report of Target using data analysis to predict which customers were newly pregnant (Duhigg, 2012). The research question I look to answer is, what is the balance between a seamless system behavior and the need to alert a user about potential privacy loss, and what design principles are relevant to this problem (Satyanarayanan, 2001)?

Conclusion:

With an estimated five hundred percent increase in the number of devices connected wirelessly, National Instrument believes that the Internet of Things is the front runner for the next technological wave (National Instruments, 2015). My technical research and my tightly coupled STS research both look to provide a better understanding of where societies' privacy concerns will go in the near future.

References

Duhigg, C. (2012, Feb 16) . How Companies Learn Your Secrets. *The New York Times.* Retrieved from: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0

Hanson, J. (2015, Aug 22) . Controlling the Physical World with Leap Motion and Raspberry Pi. Retrieved from: http://blog.leapmotion.com/controlling-physical-world-leap-motion-raspberry-pi/#more-6158

National Instruments. (2015) . *NI and the Industrial Internet of Things*. Retrieved from: http://www.ni.com/internet-of-things/

National Intelligence Council (2008, Apr) . *Disruptive Civil Technologies: Six Technologies With Potential Impacts On US Interests Out To 2025.* Retrieved from: http://fas.org/irp/nic/disruptive.pdf

Satyanarayanan, M. (2001) . Pervasive Computing: Vision and Challenges. *IEEE Personal Communications, 8(4), 10-17.* Retrieved from: https://www.cs.cmu.edu/~aura/docdir/pcs01.pdf

Tucker, P. (2014) . *The Naked Future.* New York, NY: Penguin Group.

Wasik, B. (2013, May 14) . In The Programmable World, All Our Objects Will Act As One. Retrieved from: http://www.wired.com/2013/05/internet-of-things-2/

Wind River (2014). New Life For Embedded Systems In The Internet Of Things. Retrieved from http://www.newelectronics.co.uk/article-images/67055%5CEMS%20White%20Paper.pdf