Prospectus

Human Interactions with Rotundaur

(Technical Report)

Open Data and Privacy in a Cyber-Insecure World

(STS Research Paper)

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Edwin Sompayrac

Fall, 2019

Department of Mechanical Engineering

Signed: Edwin Sompayrac

Approved: _____ Date _____

Sean Ferguson, Department of Engineering and Society

Approved: _____ Date _____

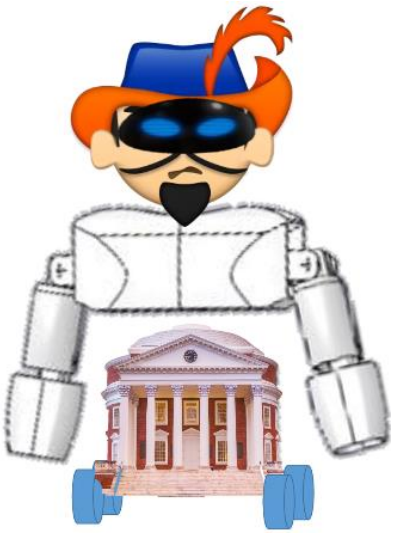
Gavin Garner, Department of Mechanical Engineering

Technical Report:

For the technical report, my capstone project has decided to build and program an interactive robot. Initially, our capstone group was going to move in a slightly different direction. There was the upper half of a robot left from a capstone project a few years ago. It had a massive torso with arms and a head, all made from aluminum, that moved with pre-programmed code. At first, we were planning on creating legs for the robot so that it could move around. Since only the torso was created, it was bolted down in the Mechatronics Lab of the Mechanical Engineering Building, unable to move around. When starting to think about a lower half system that would allow the half-completed robot to move, our group quickly hit a few road blocks. First, the upper half of the robot was incredibly heavy, meaning we would have to design a leg system that would be able to support a large, constantly moving center of mass. Next, since the top half of the robot was already created by students in the past, the leg system would half to match the theme of the already created torso, so as to make it look like one singular capstone project done by one singular group. We decided that we wanted to have full control over what a future robot would look like, and be able to use our own creativity to come up with a design that we wanted, and not have to appeal to another group. So instead, we scrapped the idea of working on the old robot and decided to build our own.

Rotundaur is currently being worked on as our new capstone project. Rotundaur is a half-rotunda, half-humanoid robot, with its name coming from the half-horse and half-man creature, the centaur, from Greek mythology. Rotundaur consists of a rotunda chassis, where the dome of the rotunda lofts into a torso of a humanoid robot. Mecanum wheels are attached to the chassis giving Rotundaur holonomic drive. Rotundaur has two arms, and will have some sort of head that is still being discussed.

When designing Rotundaur, our group felt there needed to be a facet of human interaction involved with the project in order to engage people with Rotundaur. To do this, we created arms that are able to play back any type of movement that a user input could give it. With each arm having three motors (two in the shoulder and one in the elbow) a user is able to move the arms in any way they want, and the robot will be able to play it back. This allows users to have infinite possibilities of movement and can make Rotundaur wave hello, dance, give hugs, or any other creative movement the user wants. Another cool part about Rotundaur is that it is made up almost completely of 3D printed material, meaning if a piece breaks, it could easily be reprinted and replaced.



Currently, our group has one working arm system, able to be played back, and a working wheel system. We are currently all working on Solidworks models of the torso and rotunda sections of the body. By Monday, 11/11, our group hopes to have a fully working prototype of Rotundaur moving around. Because our group is working in an accelerated capstone design class, Rotundaur will be finished by December 12th of 2019, and the technical report will be finished by December 15th, 2019.

Here is a quick picture of the concept of Rotundaur. It was important for our group to keep UVA integral to the theme of the robot. In the next month, our group plans on having Rotundaur give tours of the Mechatronics Lab or the Mechanical Engineering Building as a whole, once again to inspiring a human interaction element to the project.

STS Research:

As digital technologies converging with the physical infrastructure in smart cities, there becomes larger risks when it comes to cyber-security within the city. The number of IoT devices is expected to more than double by the end of 2020[1], creating more and more facets for cyber-attacks that can wreak havoc if cities are not prepared. As cities are becoming "smarter" there needs to be cybersecurity developments and principles installed in order to keep citizens safe and protect against the breakdown of society. Healthcare, education, power and utilities; all of which are left vulnerable if there aren't cyber-security requirements and regulations. With an increase in digitalization, there will be more data available for use within a smart city. Open data initiatives have been taken in different municipalities, locally and globally, in an effort to create more transparency in the relationship between government and its citizens. There is little debate about the potential benefits of open data in a city, but how can smart cities use open data effectively, while keeping the data and the privacy of its citizens secure? Using value sensitive design with a social constructivism of technology framework, engineers and government entities can begin the process of delivering a solution to open data needs while preserving integrity of the privacy of its citizens.

Technology and Privacy have long been intertwined. When google launched Google Glass in 2013, the lines between privacy and technology were blurred even more. Some businesses even declared "Glass-free zones"[2] as there were concerns that the embedded video camera was an invasion of privacy of the clients patronizing the establishment. As the influence of technology accelerates in society, the definition of privacy becomes messier. The technomoral

[1] Pandey, P., 'Making Smart Cities Cybersecure' (April 11, 2019);
[2] Kudina and Verbeek, 'Ethics from Within: Google Glass, the Collingridge Dilemma, and the Mediated Value of Privacy' (Page 8)

impact[3] of new technologies that collect data indicate a dynamic privacy definition, that currently has no concrete foundation in today's smart cities. With the average person in America owning 8 IoT devices[4], new technologies that utilize and share data affect the security and privacy of every individual in a smart city.

Open data and information isn't a new concept. In 1967, the Freedom of Information Act (FOIA) was passed which provided the public the right to request access to records from any federal agency.[5] This excludes certain information about national security, public safety, and certain personal information. However, for the most part, if the record exists in a federal agency, any member of the public can request to access the information, and can be granted access to the information.

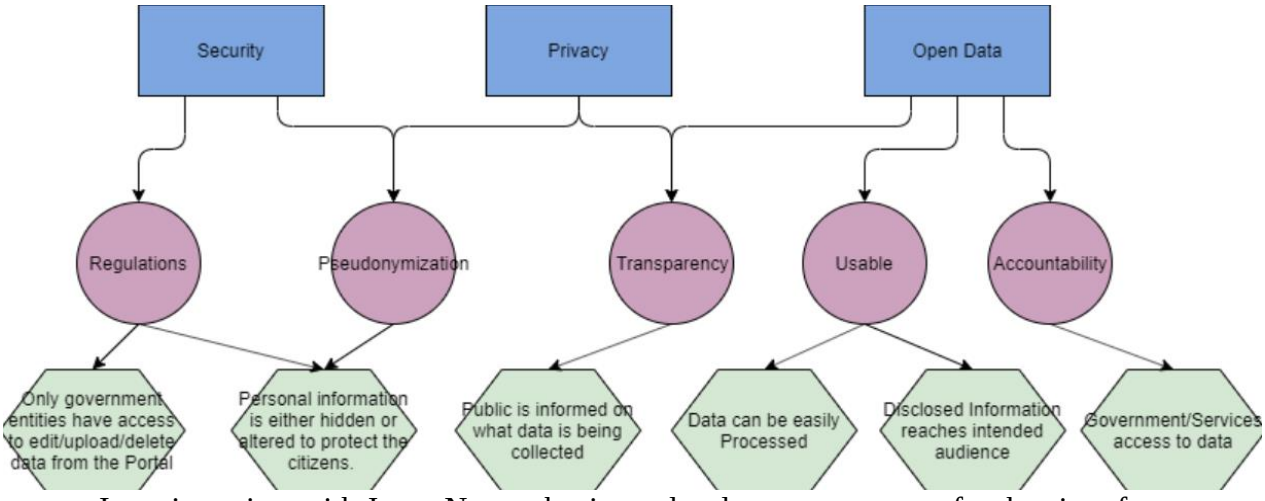
When Michael Signer was elected as the Mayor of Charlottesville in 2016, he decided to hold an open "office-hours" for the people of Charlottesville to come meet him and talk about what they would like to change about the city.[6] From the office hours, there was an overwhelming amount of support for the creation of an open data portal. Charlottesville already had GIS capability, and a lot of data was already "open", it just wasn't easily accessible. Because of the existing GIS software, no additional funding was necessary to develop the open data portal except for staff time. The social constructivism of technology (SCOT) recognizes multiple actors within the open data and security network. For this situation, actors would include citizens, government, internet, services, etc. The citizens, in their everyday lives, are producing data that engineers and city government officials can use to better the

[3] Kudina and Verbeek, Page 5
[4] 'IoT Has Quietly and Quickly Changed Our Lives' (February 1, 2019);
[5] United States Department of Justice, 'What is FOIA?'
[6] Mandel, J., 'City's open data portal goes online with hopes of creative use by public' (August 27, 2017);

community around them. As the engineers and city staff were creating the open data portal for the Charlottesville community, they could use the values that matter most to the citizens. To do this, the engineers should think about value sensitive design, in order to come up with the design requirements that serve the citizens values.

Value Sensitive design is a way of thinking about values that are important to specific groups, and then creating norms and design requirements that come from the values. At the start of the next page is a simplified version of a value sensitve design diagram with the values on top, the norms in the middle, and the design requirements on the bottom. Using the diagram can help engineers create a system that keeps the values of the citizens at the forefront. With the Charlottesville open data portal, there was more of a focus on the open data value, and making the data usable and easily accessible.

The open data portal is broken into 10 different classifications: Property and land, economy, city operations, public safety, demographics, transportation, recreation, infrastructure, environment, and GIS base layers.



In an interview with Jason Ness, a business development manager for the city of Charlottesville and an instrumental member of the creation of the open data portal, he explained

some of the goals of the portal, as well as some of the privacy concerns that came along with it. When asked about the data that is available to the public, Ness stated that none of the data in the portal is very "personal" at all, and that every piece of information available on the portal was already FOIA-able. One example of this is in the public safety data, under a crime dataset, a member of the public is able to see the first and last name of a criminal, the crime they were charged, when, and where the crime took place. This may seem like a lot of personal information, but all of this information is available to public through the Charlottesville court system. The open data portal is merely just one place where all of the information can be easily found. When I asked Ness what the goal of the open portal for Charlottesville was, he responded by saying data scientists and members of the community can use the data to make Charlottesville a better place through data analysis. He gave two specific examples of when this was the case:

The first is an example with the free Wi-Fi on the Downtown Mall. There are multiple routers on the mall and when a new device gets connected to it, the router can see the name of the device and what time is was connected. As people walk around the mall, different routers pick up the same devices at different times, being able to "track" where and when people are moving. Data scientists are using this data to see how weather patterns on certain days affect traffic on the downtown mall as well as how events affect mall traffic. This can develop patterns of human traffic to help the businesses on the mall with a proper amount of staffing or to help people find open places to park.

The second example was that environmentalists are currently using the utility data to see which neighborhoods are using the most water and gas utilities and which neighborhoods weren't. By analyzing the data over the course of a year, there is information being uncovered about more efficient ways to wire the utility infrastructure of the city, so that neighborhoods are

able to get what they need more effectively. This could end up saving the city and the citizens thousands of dollars a year in wasted utilities. All while keeping sensitive information private.

Of course, not everything is good news about open data. Ness revealed some ways in which people who wanted to do harm could use the portal to their advantage. The example he gave was hypothetical, but intriguing. Suppose John and Jane Doe live in a nice house in a nice part of town. The portal could be used to see the home owner data. Maybe, the two of them bought the house in 1980 so they're both on the record as owning the house but, in 2010, the ownership changes to just Jane Doe. A criminal could see all of this and assume that Jane is an older woman, living alone, and in a nice house in a nice neighborhood. A person with malicious intent could see this as an opportunity to strike. While there are no reports of this happening, Ness admitted that it is a sad possibility with the open data portal. He also reminded me that all of that information would be FOIA-able, however the portal makes that data easier to access.

There is still a lot to be discovered when it comes to open data and the privacy of citizens. Cities are modernizing at a rapid rate, and technomoral implications of the digital age are still being discovered. It is clear that no municipality has perfected the technique of keeping data secure, and at some point, it all comes back to keeping the data *physically* secure. Ness continually said that it is relatively easy to get into a government office, and it only takes one open laptop by a government employee to access loads of sensitive and private data. The research will continue to focus on Charlottesville and ways to increase the amount and usefulness of the open data while also increasing the security of citizens.

Bibliography:

Carolan, L. (2016). Open data, transparency and accountability: Topic guide. Birmingham, UK: GSDRC, University of Birmingham. Retrieved from https://assets.publishing.service.gov.uk/media/5857fdcb40f0b60e4a0000d6/OpenDataTA_GSDRC.pdf

(FOIA), F. of I. A. (n.d.). FOIA.gov (Freedom of Information Act) Frequently Asked Questions (FAQ). Retrieved from https://www.foia.gov/faq.html.

IoT Has Quietly and Quickly Changed Our Lives. (2019, February 1). Retrieved from https://www.ncta.com/whats-new/iot-has-quietly-and-quickly-changed-our-lives.

Joo, J. Y.-M., & Lee Kuan Yew School of Public Policy. (n.d.). Smart Cities: A New Age of Digital Insecurity. Retrieved October 10, 2019, from https://iiss.tandfonline.com/doi/full/10.1080/00396338.2018.1448577#.XZ9gXEZKg2w.

Making smart cities cybersecure. (n.d.). Retrieved October 10, 2019, from https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html.

Mandell, J. R., Woods, C. R., Robinson, E. undefined, & Hays, E. undefined. (2017, August 27). City's open data portal goes online with hopes of creative use by public • Charlottesville Tomorrow. Retrieved from https://www.cvilletomorrow.org/articles/charlottesville-launches-website-for-open-data.

Millennials Throw Caution to the Wind Regarding Internet Security. (n.d.). Retrieved from https://securethoughts.com/younger-generations-throw-caution-wind-internet-security/.

Vaughan, F., & University of Birmingham. (2017, October 24). Open Data, Transparency and Accountability: Topic guide. Retrieved October 10, 2019, from https://opendatacharter.net/open-data-transparency-accountability-topic-guide/.