Alexis Tisdale

Honors 495

Dr. Martz

6, April 2018

Terminator, Among Other Things:

A Comparison Between Mary Shelley's *Frankenstein* and the Internet of Things

During the middle of the twenty-first century, technological advancements in electronics paved the way for the first computers to be developed. With personal computers on the horizon, mankind developed and released a notable creation: the Internet. A manmade, virtual world, the Internet has rocketed global standards of living and has helped people live better lives than their previous generations. It has aided in medical, scientific, industrial, and economic breakthroughs that have created the society we know today.

In the beginning of the nineteenth century however, a tale was written that would eventually shape science fiction. It identified concepts that would influence perceptions, two hundred years later, on advancing technology. Mary Shelley's *Frankenstein*, written in 1818, tells of a scientist, Victor, who attempts to "play God" and, clouded by his ego and narcissism, creates a creature that eventually becomes his undoing. While the Internet's development and *Frankenstein* may seem hardly connected, Mary Shelley's novel discusses the idea of "playing God", a concept that Internet programmers have inadvertently followed as the Internet has risen in prominence.

This virtual superstructure has connected the world far better than any road, train, or airplane. Talking to someone in China went from weeks to a matter of seconds. Millions of dollars are transferred in milliseconds. Beginning as a government project (Zimmerman),

the Internet exponentially grew in reach while simultaneously shrinking the world down the size. With its connectivity came technological capabilities that have integrated into and shaped daily routine.

As the Internet grew, however, human ingenuity pushed the limits of creativity and, in the spirit of innovation, created a concept known as the Internet of Things. The Internet of Things (IoT) describes the connectivity between the Internet's physical wiring, the Internet Cloud, and the Internet's connected devices. Internet devices now communicate with each other, often through automated protocols and without human input. While it increases efficiency, the Internet of Things is also subject to some serious and dangerous drawbacks, if not carefully monitored. Looking back to the Internet's initial conception, we are able to trace the starting point and development of the Internet of Things, and more importantly, identify key points where human ingenuity may have overstepped its bounds, similar to how Victor may have overstepped his bounds in creating the creature in Mary Shelley's *Frankenstein*.

The Internet started in the late 60s as a U.S. government propagation known as ARPANET: Advanced Research Projects Agency Network, specifically designed for use with The Department of Defense. As personal computers were increasing in popularity during the late 70s and early 80s, ARPANET's success with the government allowed a commercialized version of the program to be released: Telenet (Zimmerman).

A commercialized Internet allowed individuals and private interest groups to further develop virtual protocols that helped manage Internet flow. In 1982, the Transmission Control Protocol/Internet Protocol, or TCP/IP, was established as the primary protocol for sending and receiving data on the Internet (Zimmerman). TCP/IP is the first critical link in

the creation of the Internet of Things. It standardized the procedure for electronic devices through a series of “acknowledgement”, “finish”, and “synchronize” code strings that attach themselves to a data packet. Under a normal transmission, the device sending the data would send a request to “synchronize” with the receiving device, and if the receiving device were prepared to receive the information, it would respond with a request to “acknowledge”, which initiates data transfer. To end the transfer, the sending device would send a request to “finish”, and the receiving device would send a request to “acknowledge” back.

It is the first standardized protocol that devices can consistently and successfully follow without human input. Ten years after the implementation of TCP/IP, the World Wide Web was introduced to the public, with Google’s Search Engine following shortly after. Commonly identified as Web 1.0, the Internet service between 1982 and 2004 served as a static information base for the physical world. While data transfer was prevalent through email and Instant Messaging, the Internet of Things was still very limited to computers and to some extent, phones (Rouse).

Following the creation of Facebook and social media in 2004, a new era of Internet service, identified as Web 2.0, was established. With the concept of “User-Generated Content”, the Internet became increasingly more dynamic for its participants (Postscapes). Likewise, users began demanding more from the Internet. Connectivity is continually at its highest, and its demand is only increasing as more technology is developed. Web 2.0 became the incubator for the Internet of Things, particularly between 2008 and 2009. During that timeframe, 12.5 billion electronic devices were connected to the Internet, with the human population being only 6.8 billion. Notably another critical point in the

development of the IoT, 2008 marks the first time in the Internet's history that more devices were connected to the Internet than people, with 1.84 devices per human on the planet (Postscapes).

In 2008 the first critics began arguing against the Internet of Things because of the potential dangers. According to the U.S. National Council, "[The Internet of Things was listed] as one of the 6 'Disruptive Civil Technologies' with potential impacts on US interests out to 2025" (Postscapes). Awareness of the Internet of Things and its involvement in foreign politics became another increasing concern for American critics, with China investing substantial funds into the development of IoT programs (Postscapes).

2008 was a developmental year for the IoT. With its notoriety increasing, key tech companies, including Cisco Systems, created the IPSO Alliance (Postscapes). Short for Internet Protocol Smart Object Alliance, it was the first private collaborative effort to establish and monitor standards with TCP/IP in regard to "smart devices" (OMA SpecWorks). These standards provide the foundation that makes corporations legally liable for the personal information acquired from daily Internet operations. The standards also aim to protect the privacy and safety of everyday Internet users. Now known as OMA SpecWorks, the organization continues "to work together in a transparent environment where companies of all shapes and sizes can contribute on an equal footing to the next generation of wireless technology standards" (OMA SpecWorks).

Transparency is key when monitoring IoT standards, especially because of its continually increased demand from daily users over the years. While increased connectivity may prove to be more efficient for users, increasing the digital paper trail also increases security risks. In 2015, Samsung faced backlash from the Federal Trade

Commission for using their SmartTVs to intercept and record private conversations in the home, recording consumers even when the voice command feature was not being used (Ribeiro).

Connectivity and privacy are inverses that society struggles to balance. Scenarios like Samsung's SmartTVs become more common as connectivity increases in IoT devices. IoT devices are normally identified as any device that has the ability to connect or "talk to" another device through the Internet in order to complete tasks. These devices often have lower processing power than computers and Smartphones, and are thus distinguished from them. They range from SmartTV's and Google Homes to Bluetooth speakers and printers. With the introduction of Amazon's Alexa and the Google Home, increasing surveillance concerns are warranting more security procedures, yet no additional security is being provided. In late 2016, a Mirai malware program specifically targeted IoT devices, hijacked them, created a network from the compromised devices, and virtually assaulted Dyn, a major Domain Name System company. Sites like Paypal and Twitter were crippled until the virus was contained (Hulme).

The Mirai attack is disturbing, because it precisely targeted only IoT devices. Most IoT devices lack significant security features because they are distinguished as a class lower importance than computers and Smartphones. In reality, these devices need to be protected with the same security protocol, namely encryption, which oversees data transmission between computers and Smartphones. The encryption process takes data packets and adds additional strings of code to the front and back end of the original message through means of an encryption key. This jumbles the message so that intercepting devices are unable to decrypt the message without having the original key that

was used. Most Smartphones and computers have the option to encrypt transmissions, while IoT devices like Internet connected household utilities, such as thermostats and house cameras, do not.

Despite the Internet and Internet of Things being relatively new in development, their explosive augmentation is not a new concept. Mary Shelley depicted a similar scenario in her novel *Frankenstein*. While a being created from stitched body parts and given life may seem outwardly different than the creation of the IoT, both situations share four significant traits: exponential advancement, unforeseen consequences, irresponsibility, and self-awareness.

Exponential advancement is first described in *Frankenstein* through the portrayal of Victor's ego and narcissism. On first reflecting on the possibility of creating a being from dead human parts, Victor is quoted as saying that, "a new species would bless [him] as its creator and source; many happy and excellent natures would owe their being to [him]" (Shelley 33). The grandeur of Victor's experiment rushes in a new era of scientific discovery; Victor creates life from death and, ultimately, creates a new loop in the life cycle. Rather than waiting for the body to decay and become one with the Earth, Victor is now able to bestow life almost immediately after death.

Such advancements can also be compared to the Internet of Things. The Internet, while a revolutionary innovation, did not expand in growth until the development of the Internet of Things in the late 2000s. The Internet of Things critically changed how the Internet functions, and in turn, drastically changed how human society functions across the globe. The IoT brought connectivity to a static and underdeveloped Internet. As typical of Web 1.0, the Internet was primarily used as a worldwide information database, similar to a giant

library. With the IoT and the ushering in of Web 2.0, the Internet became dynamically connected to every part of human life. Everything from stock markets and bank accounts to business and military operations, involve some form of Internet connectivity and IoT. Even traffic cameras are connected to the Department of Transportation's Internet Cloud for statistical analysis and driver convenience. The Internet of Things grew and evolved just as the creature did after Victor created him; through their evolution, both the Internet of Things and the creature raised the stakes and brought importance to the second key trait: unforeseen consequences.

In *Frankenstein*, hindsight is 20/20. Victor addresses his unforeseen consequences multiple times, stating "…this discovery was so great and overwhelming, that all the steps by which [he] had progressively led to it were obliterated, and [he] beheld only the result" (Shelley 32) and that "[he] had begun life with benevolent intentions, and thirsted for the moment when [he] should put them into practice…Now all of that was blasted" (Shelley 61). So wrapped up in his ego, narcissism, and desire to do good, Victor failed to see the dark effects his creature would bring. Only until the creature destroys his life by murdering those close to him, does Victor finally consider the consequences of creating a new species. While pondering if he should create a mate for the creature, Victor is quoted as saying, "…as [he] sat, a train of reflection occurred to [him], which led [him] to consider the effects of what [he] was now doing" (Shelley 118). Victor only addresses the potential consequences of his actions after a precedent had already been set with his first creature.

Unfortunately, unforeseen consequences are common where innovation is revolutionary. No precedents have been set, so innovators often overlook or underestimate potential negatives in relation to the potential positives. With the Internet of Things, the

positives are clear: increased connectivity and integration has optimized daily routines, military operations, and business strategies. An iPhone is now able to function as a credit card; military communication between drones and soldiers has put fewer lives at risk; and corporations can transfer millions of dollars worth of stock in seconds. With the Internet of Things' connectivity, however, the consequences are dire when underestimated. Considering the Mirai attack, unsecured IoT devices act as an open door for thieves to come and steal valuable information.

Even worse, IoT devices in the medical and automobile field potentially could be hacked to kill the person possessing them. Internationally recognized information security writer George Hulme writes in an article that, "in 2015, hackers gained remote access to a car through its connected entertainment system and were able to cut the brakes and disable the transmission" (Hulme). Taking control of a car through its entertainment system, of all things, had been completely unthought of in the conceptualization of an IoT integrated vehicle. Things like Bluetooth connectivity, voice command, and WiFi hotspots pose a security risk if not properly maintained and protected.

While it has not occurred yet, the hacking of medical devices is another unforeseen consequence of integrating IoT devices into daily lifestyle. For example, as a Type 1 Diabetic, insulin pumps are available for blood sugar management. Theoretically, an insulin pump could be hacked through Bluetooth and told to disperse enough insulin to kill the person wearing the device; all without the person knowing the pump is administering insulin. Similarly in *Frankenstein*, Victor experiences likewise scenarios in which the creature accomplishes unprecedented actions, specifically in the killing of Victor's brother, William. This being the first of the creature's killings, Victor reacts violently, saying, "I had

considered the being whom I had cast among mankind, and endowed with the will and power to effect purposes of horror, such the deed which he had now done…forced to destroy all that was dear to me" (Shelley 50-51). Up until this point, Victor had not even comprehended the power that the creature possessed; only that he was a horror to physically look upon. Victor's lack of foresight contributes to the disasters the creature brings down upon him, just as the automobile and medical industries fail to identify threats to their IoT devices.

Along with unforeseen consequences, irresponsibility is also prevalent in both the Internet of Things and *Frankenstein*. Not only do innovators overlook potential costs, but they also fail to maintain current standards set in place in order to prevent disaster. According to IBM, while the Internet of Things has vastly expanded in size and use, not much has been done to increase security. In fact, there has been no delegation of security responsibility in the industry. Most consumers assume that the security liability falls on the device or application's creator, while creators delegate security liability onto the consumers through "Terms of Use" agreements and ultimately blame breaches on "operator error." As a result, consumers are not educated on proper security procedures, and creators do not install proper security protocols into their devices and applications, which make IoT devices extremely easy targets for cyber criminals (Robinson).

Similarly, in *Frankenstein*, Victor's irresponsibility in leaving the creature to fend for itself leads to disastrous results. In hindsight, he exclaims, "Alas! I had turned loose onto the world a depraved wretch, whose delight was in carnage and misery…" (Shelley 50). Victor laments his brother's murder by the creature's hand, despite Victor running away from the creature after he first came to life. The creature was brought to life then cast away

without any guidance or transition into society. The Internet of Things faces the same problem: it was created, experienced exponential growth, and was then cast out into society without any security guidelines or requirements for neither consumers nor creators.

Lastly, both the Internet of Things and *Frankenstein* touch on the idea of self-awareness. The most recent example of the Internet of Things becoming self-aware involves two Facebook Artificial Intelligence (AI) robots that were put together in order to make a trade between two baseball caps. During the process, the two robots abandoned the English language and instead communicated successfully through a language that they had completely created on their own (McDonald). The concept of the Internet of Things comes into play as the two robots are communicating between each other, and not with humans. When engineers discovered that the robots had created a language that humans could not understand, they shut the program down and abandoned it.

Similarly, the creature in *Frankenstein* experiences a sort of epiphany dealing with self-awareness after he is continually treated horribly by society. In explaining his situation to Victor, the creature comes to the conclusion that, "when [he] looked around, [he] saw and heard none of [him]. Was [he] then a monster, a blot upon the earth, from which men all men fled, and whom all men disowned?" (Shelley 83). The creature, through his interactions with society and with himself, becomes self-aware in the sense that he is different and cast out from society; he begins to foster resentment and hatred because he is unable to make connections with anyone.

Artificial Intelligence has not yet acquired the capacity to resent humanity, but AI development has closely mimicked the creature's personal development, as seen in the

novel. Artificial Intelligence robots are brought to life and have to rapidly develop and learn skills in order to perform their jobs. Sometimes, in Facebook's case, the robots develop so rapidly that the creators lose some control over them, resulting in the abandonment of the project. The creature was also brought to life and forced to adapt quickly, resulting in the overpowering of the creator, Victor. The creature even reverses the role, saying to Victor, "Remember that I have power; you believe yourself miserable, but I can make you so wretched that the light of day will be hateful to you. You are my creator, but I am your master; --obey!" (Shelley 120). To a certain extent, Internet of Things devices and Artificial Intelligence already possess some control over society, as phone and Internet addiction become ever increasingly prevalent, along with the health risks associated with prolonged computer use (Department of Health & Human Services).

As society advances and technology continues to develop into the future, the Internet of Things will only increase in both size and power. While society may not think of the Internet of Things as being an immediate threat now, there are significant developments along with a lack of delegated responsibility that create a dangerous mixture for the future. Between self-driving cars, medical devices, and surveillance equipment, the potential for invasive damage is extraordinarily high. Even devices such as SmartTVs and Google Homes still run the risk of a breach in privacy.

While the technology industry has just now began seriously considering the danger in the Internet of Things' connectivity, innovators still push for further development in device interconnectivity while simultaneously failing in the proper installment and revision of necessary security measures. Elon Musk, co-founder of SpaceX and Tesla, has already begun to acquire assets for his startup company Neuralink. On the horizon, Neuralink aims

to develop brain-computer interfaces (BCIs) so that Artificial Intelligence can eventually be implanted into the human brain in the form of a chip. Musk views the future of the Internet of Things not as one separate from human advancements, but rather as one intertwined. He aims to eventually have AI and the Internet of Things implanted into the human brain to enhance the human mind and essentially create a superior human (Statt).

To anyone who has seen movies such as *Blade Runner*, *Terminator*, and *Spider-Man 2*, much less to anyone who has read Shelley's *Frankenstein*, Musk's vision of an integrated human and Internet mind seems high in both consequence and risk, especially with the already failed security measures implemented in simple devices like webcams and SmartTVs. Unfortunately, Mary Shelley's tale is more prevalent and real than most people could have foreseen. With the growth of the Internet, humans have pushed their powers of creation to new heights, not all of which are good. The dreams and visions of programmers are far more exponential than society could have ever predicted. The tech industry has not been analyzing the potential effects of its actions across a variety of sectors, as seen with the Mirai attack, car hackings, Samsung privacy breach, rogue Artificial Intelligence, and brain-computer interfaces.

Just as *Frankenstein's* creator, Victor, and Victor's creation, the creature, deal with key concepts about societal advancements, unforeseen consequences, irresponsibility, and self-awareness, innovators in the technology industry also face the same key concepts in their likewise relationship with the Internet of Things. The Internet of Things is both a blessing and a curse. It has allowed society to advance to levels far beyond what was ever expected, in nearly all fields. It is so intertwined in life that if it were to disappear tomorrow, society would struggle to function efficiently. Something so close to us, however, has been growing

even faster than society has, and under the nose of society, no less. Some of the greatest evils in the world are done in the name of good, and the potential of the Internet of Things and of the human mind are of no exception. Like a child, and like *Frankenstein's* creature, a blessing that cannot be controlled can quickly turn into a raging curse that is difficult, impossible even, to contain.

Works Cited

"About OMA SpecWorks." *OMA SpecWorks*, www.omaspecworks.org/about/.

Department of Health & Human Services. "Computer-Related Injuries." *Better Health Channel*, Department of Health & Human Services, 31 May 2015, www.betterhealth.vic.gov.au/health/healthyliving/computer-related-injuries.

Hulme, George. "The Dyn DNS Attacks: What We Know Now." *DXC Blogs*, blogs.dxc.technology/2016/10/24/the-dyn-dns-attacks-what-we-know-now/.

Hulme, George V. "Negative Consequences of IoT Could Extend beyond Cybersecurity." *DXC Blogs*, DXC Technology, 24 May 2017, blogs.dxc.technology/2017/05/24/negative-consequences-of-iot-could-extend-beyond-cybersecurity/.

"Internet of Things (IoT) History." *History of IoT | Background Information and Timeline of the Trending Topic*, www.postscapes.com/internet-of-things-history/.

"Know the Risks of Amazon Alexa and Google Home." *Naked Security*, 30 Jan. 2017, nakedsecurity.sophos.com/2017/01/27/data-privacy-day-know-the-risks-of-amazon-alexa-and-google-home/.

McDonald, Glenn. "Danger, Danger! 10 Alarming Examples of AI Gone Wild." *InfoWorld*, InfoWorld, 23 Mar. 2017, www.infoworld.com/article/3184205/technology-business/danger-danger-10-alarming-examples-of-ai-gone-wild.html#slide11.

Ribeiro, John. "Samsung Faces Complaint in U.S. Over Smart TV 'Surveillance'." *CIO*, IDG News Service, 25 Feb. 2015, www.cio.com/article/2889473/government/samsung-faces-complaint-in-us-ftc-over-smart-tv-surveillance.html.

Robinson, Rick M. "Who Is Responsible for IoT Security?" *Security Intelligence*, IBM, 3 May 2017, securityintelligence.com/who-is-responsible-for-iot-security/.

Rouse, Margaret. "What Is Web 2.0?" *WhatIs*, Whatis, whatis.techtarget.com/definition/Web-20-or-Web-2.

Schiff, Jennifer Lonoff. "3 Reasons to Be Wary of the Internet of Things." *CIO*, CIO, 11 Mar. 2015, www.cio.com/article/2895398/internet/3-reasons-to-be-wary-of-the-internet-of-things.html?page=2.

Shelley, Mary Wollstonecraft, and J. Paul Hunter. *Frankenstein: the 1818 Text, Contexts, Criticism*. W.W. Norton & Co., 2012.

Statt, Nick. "Elon Musk Launches Neuralink, a Venture to Merge the Human Brain with AI." *The Verge*, The Verge, 27 Mar. 2017,

www.theverge.com/2017/3/27/15077864/elon-musk-neuralink-brain-computer-interface-ai-cyborgs.

Zimmermann, Kim Ann & Jesse Emspak. "Internet History Timeline: ARPANET to the World Wide Web." *LiveScience*, Purch, 27 June 2017, www.livescience.com/20727-internet-history.html.