Jack Shirley

Professor Madden

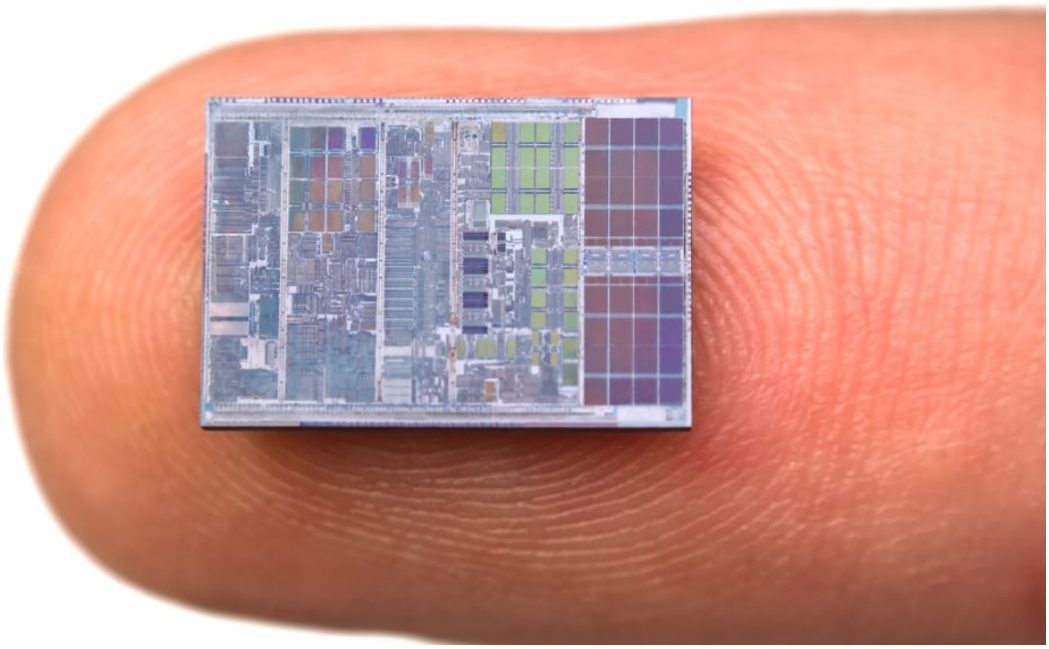
EMCS 2800

1 March 2020

Human Microchipping: Simplified Technology or Privacy Risk?

For almost 25 years, pet owners across the world have begun implanting their animals with microchips. This miniature piece of hardware allows an animal to be properly identified when it goes missing. As humans, the digital landscape continues to evolve and consumer demands for more efficient access and payment are growing, with a tremendous focus on making the user experience faster and better. There has been a migration from PCs to laptops, laptops to mobile devices, and today, users are able to execute commands through wearable technology. But what if human microchips could enhance our everyday digital experience? I have delivered interviews to several leaders in the human microchip market, to gain perspective on specific problems this technology can help solve and where it could create a cultural backlash. The results were unexpected, and since the inception of my research, there has been new state and global legislation to preserve human rights and disallow this practice. There has also been increased adoption across the private sector for microchips, and certain countries have begun standardizing on microchipping methods as a primary protocol for daily tasks. The objective of this paper is to prepare the reader for the paradigm shift that is currently happening, and through predictable measures, facilitate a discussion that explains which communities this technology can positively impact, and which ones will resist. By providing some context into the security and privacy challenges of the actual integrated circuit of a microchip, you will be able to quantify the balance between usability and personal protection, and what your appetite for risk will be.

To build up microchipping, we need to first breakdown what this technology does, and how it first helped living animals get identified. A microchip is an integrated circuit that consists of a transponder (often called a tag,) memory and a controller. Jack Kilby of Texas Instruments and Robert Noyce of Fairchild Semiconductor Corporation were instrumental in the creation of the first microchip and received a U.S. patent in 1959. A few years later, the U.S. Air force implemented microchips into ballistic missiles in order to improve guidance systems. NASA later purchased microchips to aid the Apollo project (Bellis.)



Fawcett

We did not begin to see mainstream use cases for RFID until the 1980s, when RFID tags were utilized to track bar codes for inventory and in supply chain operations. The most common RFID systems run off a passive ultra-high frequency (UHF) and scan a tag from up to 10 feet away. Since the tag has no internal battery, it gets powered when interacting with radio waves coming from an RFID reader. They are compact, relatively inexpensive and the most common.

Active RFID tags require an internal power supply, and this is basically due to read range. Active readers can read tags up to 1500 feet away (What Is an RFID Reader's Maximum Range,) and since the data is transmitted through radio waves, the tag isn't required to be line of sight. All connections, passive or active, are established wirelessly.

The microchips used for living things today all contain passive RFID, so they don't need to be charged like an iPhone or a smartwatch, rather it comes alive when it interacts with the reader. RFID is still being used widely for tracking and tracing purposes too. When people run a marathon, there is an RFID tag that can be attached to the bib. Scanning attendee badges at a conference is another way to have data imported into your smartphone. Many vendors are also leveraging RFID for products in a store by replacing barcodes with RFID tags, since barcodes are more vulnerable to replication because it's just ink on paper. By placing an RFID reader near the entrance of a store, employees are alerted if a shopper was trying to steal something (Goodrich and Tamassia.)

NFC, which stands for near-field communication, is another protocol that allows two systems to interact with another. At a macro level, RFID and NFC are very similar, but NFC is engineered directly into a product designed to be read by a mobile device. When people use smart pay apps to purchase goods and services, NFC facilitates these transactions. A consumer can also learn more about a product by scanning an NFC enabled advertisement.

Ratna

Retailers like Nike are using NFC as part of a marketing outreach program to engage with sports fans. For example, if someone buys a Lakers or Chelsea FC jersey, there is an NFC tag on the jersey that a fan could scan to unlock gifts or other promotions. All you need is smartphone to do this (Ratna.)

Lookout Security is a mobile threat defense company that provides security for corporate-issued and consumer smartphones. Lookout, which was founded by three colleagues at USC, first designed a device to exploit vulnerabilities in Nokia devices, which were widely popular in 2005. The device was nicknamed the “Blue Sniper” and was essentially a cyber-weapon that could be aimed at someone’s phone extracting personal data due to a bluetooth vulnerability. The intent was never malicious, but more of a business case to highlight security flaws in smartphones. They actually put the Blue Sniper on display at the Academy Awards and compromised a few celebrities’ devices. They used this demonstration to help secure funding and later start Lookout. Depending on the transmitting system and variables like active or passive,

frequency and antenna location, the data on a microchip could get compromised from short and long ranges, and history has shown this (Hering.)

It's hard to determine exactly when pet-owners, cattle ranchers and wildlife managers started to adopt this novel technology. Destron Fearing is considered one of the market leaders in the implantable microchip market for animals. In 1945, they created the first market ready RFID tag for livestock, and have expanded their product line for pets, horses and even fisheries. Today the microchipping market has become more crowded and there are several vendors who develop animal microchips and manage an internal database for information stored on the microchip. The cost of the actual implant is about $40 dollars and the ongoing subscription is around $20 dollars annually. Many pet owners are seeing value in this business model compared to traditional collars because of the automation, simplicity and security for their pets.

According to Dr. George Dzendzel, who is a local veterinarian where I live, he gets his microchips from Destron Fearing, and another manufacturer named Avid ID Systems. He said the microchips get incapsulated in a glass material, so the pet won't react negatively, and when he first began implantation procedures the chip would often move around within the pet. The microchips today contain a patented BioBond anti-migration cap which prevents the device from migrating, while simultaneously releasing a polymer substance that accelerates tissue growth surrounding the microchip, which keeps the device in place. When a client agrees to have their beloved pet chipped, there is a 16-guage needle used to deliver the passive RFID implant under the skin, similar to a vaccine. Despite a rather large needle, the procedure is painless, although some owners elect to have the procedure done when the dog is neutered, and fully knocked out. The standard location for implanting the microchip is always is in the middle part of the shoulder-blades where the fatty tissue resides. This enables any Veterinarian to quickly identify

the animal, and because the implant uses passive RFID, there is no battery source and no lifecycle, thus there is never a requirement to replace the microchip (Dzendzel).

When you scan the animal, a unique identifier is displayed along with a number for the chip manufacturer, so there is still an extra hop before the owner gets notified. The unique identifier gets displayed in clear text along with the telephone number for the registry, which is basically a database containing all personal data. The microchips engineered by Destron Fearing have a temperature sensing capability that read the animal's body temperature, which would help detect diseases at an early stage. The registry stores the information for the pet, and all data is attributed to the unique ID. The service is 24/7, so when a clinic or animal shelter call in, they provide the unique ID number in exchange for the telephone number of the pet owner or local veterinarian clinic, and the reunion is initiated.

In order to find out which data types get stored in this backend database, I decided to engage in a little social engineering experiment myself. Our family does not own an animal, but I pretended to be a new homeowner who was in the preliminary phase of figuring out whether to have our new dog chipped or to just buy a collar with a physical ID tag. The North America website redirected me to HomeAgain, which is a company focused on pet recovery services and white labels the actual hardware from Destron Fearing. The woman I spoke with provided a high-level overview on what's included in the service. Access to 24/7 recovery specialists, lost-pet push notifications to your phone, and travel services if the pet gets recovered outside of a 500-mile radius were all part of their premium package.

I started to drill into what information is actually stored in their pet recovery database, and it was actually more than I thought. Each pet was allowed to have 4 different owner contact profiles, which included home address, email, telephone numbers and local veterinarian

information. I probed about how secure this information was, and how they actually verified people calling in with an animal's unique identifier. It was reassuring to discover that the contact information could only be released to an authorized vet clinic or animal rescue shelter, and not some random person who just purchased the latest Global Pocket Reader Plus, which can read and store up to 3,000 microchips! I created a profile on a website called Allivet, which is an online pet pharmacy, and was able to add this to my cart and proceed to the purchase window before I aborted. It's a privacy concern to discover that these types of devices are available for public consumption without any verification of working in the animal services industry. If pet recovery specialist at HomeAgain was deceived through a social engineering attempt, and did provide owner contact information, an attacker could then steal the pet since the address is known. Having this basic PII data could then lead to more complex identity theft if the attacker had financial motivation or was even trying to an obtain a prescription.

Regardless if an RFID chip was implanted into an animal or human for identification purposes, the privacy procedures and security of the device still seem to be in early stages. This is largely due to the fact that most attackers aren't considering people as a target to steal confidential information. It would take a highly motivated and deranged attacker to want to scan an animal's RFID tag and begin an attack cycle towards a human pet owner, but this scenario could happen.

One of the first human microchip use cases I began to explore was people suffering from dementia. Dementia is a clinical syndrome that impacts a person's ability to remember, and they can inevitably go missing. Microchips have been proposed as a solution to augment the search if someone with this condition does wander off, and it has the same technology as the animal implants. Most senior citizens who are approaching the twilight period of their livelihood are not

necessarily concerned with privacy issues or really technology in general, and there have been multiple requests for a streamlined implementation process to put microchips into those who suffer from this disease, which is helping early microchip startups secure funding.

Babies who are switched at birth, may seem like a fictional plot concept that could only happen on a soap opera, but it's another real-life concern for many new parents. If a microchipping procedure happened immediately following a pregnancy, it could eliminate any possibility of the child being swapped or wrongfully identified, regardless if the intent was malicious or an error by one of the nurses. Overly cautious parents are exploring microchip technology to prevent kidnapping too. Todd Morris, who is the CEO of Brickhouse Security, a surveillance security company, said he would receive at least 2 phone calls per day asking if their services included microchipping children (Taylor.)

The child microchipping use case seems controversial, but it's really the easy button compared to other wearable GPS devices on the market that a child could easily remove. Most parents I spoke with, who have a wireless family sharing plan through their carrier, will have the "Find My iPhone" feature enabled so they have visibility into their teen's whereabouts. If you are looking for 3rd party app solutions that have more robust tracking features than what you already get with iOS or Android, there are apps like FollowMee, which will provide a holistic view of where all your family members are, and even setup alerts when they go too far. This is accomplished through a feature called geofencing, and it has actually helped prevent kidnapping situations.

The popular TV show, Black Mirror, had an episode titled "Arkangel," where a daughter of a single mother has a microchip implanted in her daughter after a she nearly goes missing as a toddler. The chip could pixelate images that a child might see, such as acts of violence, sex or

narcotics (Arkangel.) Eventually the daughter begins to rebel against the mother, and the episode reveals the dark reality of what could happen when parents are tracking their children. The microchipping concerns today primarily revolve around the security and privacy of your identity, but the Black Mirror episode allowed us to experience a dystopian type of society where microchip technology could influence our basic cognitive abilities to process situations and react accordingly.

While this concept may seem hyper-progressive, it could be right around the corner. In July of last year, Elon Musk announced plans to start a new company that would develop implants for people who have brain diseases. The microchip would be implanted into a person's brain and will be able to communicate to a back-end user interface, with the goal of improving brain conditions by feeding electrical signals from neurons into the interface. The technology is still in its infancy and can't deliver any actionable remediation to the brain, but the company has ample funding, and a lot of smart researchers looking to revolutionize human enhancement practices (Martin.)

While human microchipping still seems like a futuristic concept in the United States, there are other communities around the world who have embraced this minimalist approach in order to optimize their digital surroundings. People who follow the microchipping industry consider Sweden to be the birthplace of the microchipping movement and often refer to the practice as biohacking, which is basically self-improving their own body through technology. Sweden has always been considered to be the most progressive out of the Nordic countries, and there are even plans to migrate to a society that would operate solely on digital currency, which could allow citizens with microchips to transact without ever having to insert a credit card or exchange cash.

To gain a deeper understanding on Sweden's microchip growth, I conducted an interview with Biohax CEO, Jowan Osterlund, whose company has helped drive microchipping adoption by organizing "chip parties", where Jowan himself implants the chips into brave Swedes. Jowan didn't have the typical career path that landed him in this industry. He was a body piercer for almost 15-years and was more interested in extreme sports and playing video games as a youth. But he had a keen interest in science and even had friends whom wrote some of the linux kernel modules. From the way our conversation went, he was fascinated with innovative concepts entering the market like blockchain and artificial intelligence. Given his background as a body piercer, and knowledge into the world of tech, he developed a particular interest into the intersection of humans and technology, and how a small RFID microchip could enhance our digital experience. The way he looks at it, everyone has a choice on how we choose to interact digitally.

Most people today have smartphones, but many of us are now moving towards wearables like the Apple and Samsung watches. Ten-years ago, Fitbit made a big splash by introducing activity trackers and other devices which could collect basic health data. Since then, smartwatches have activated similar functionality to that of a smartphone, and you can even call and text, as long as you have a cellular plan activated. You literally can leave the house with just your watch and make payments, get access into buildings and communicate through the same protocols used on your smartphone. Jowan believes that an implanted chip is a similar choice to wearing a watch or carrying a phone, and that future microchips will carry the same processing power as market ready smartphones today. Biohax has a vested interest in consumers choosing microchips over wearables, but ultimately Jowan believes in sovereign identity and the user controlling their digital self. (Osterlund.)

Jowan mentioned that he is also an advisor to another microchip business venture that was initially called Embedded and has just recently changed names to Mediscan. While much of the core technology under the hood remains the same, the target use case is for first responders to identify victims by scanning their microchip implant. I had a discussion with Peo Stromberg, who is the acting CEO & Founder at Mediscan from his home in Malta to get an overview on the company's mission. "We are experimenting with sensors to detect different blood and stress levels. We still want to protect the digital integrity of our users, but we want these devices to be more active than passive" (Strömberg.)

Mediscan's goal is to provide microchips that can detect DNA, heartrate and other internal irregularities, and then alert a caregiver or family member. If a medical team responds to a car accident, they are already working with an aggressive timeline to revitalize a patient and provide sufficient medical care. But if a victim is wearing a microchip, it could dramatically accelerate the treatment process, similar to those who have to wear diabetes' bracelets. In the previous experiences I've had working with healthcare, the culture among physicians and caregivers is always life and death, and technology often gets in the way, but if wearing a microchip enabled medical staff to provide faster and more efficient treatment, then more lives could be saved.

Mediscan has also signed an agreement with the largest camel racing league in Dubai to monitor blood levels and banned substances that could be injected into the animal. The Mediscan microchip would be able detect a drug like dexamethasone, which would get injected into the camel's vein to enhance racing performance (Al-Nuaimi.) Peo and I also explored how a microchip in an athlete's body would improve how organizations monitor for performance enhancing drugs. The Union Cycliste Internationale (UCI) is the governing body for all

competitive cycling including the Tour de France. There is no systemic review process to observe if a cyclist has been doping or not. The tests that get delivered are manual and random. If a pro cyclist had a microchip though, officials could easily detect if hematocrit levels, which is the volume of red blood cells, was unusually high. This would most likely indicate that the cyclist was involved in an illegal doping program. But cyclists would still have to comply with having an implant inside of their body, so there would be no method to achieving general governance if microchipping athletes remains voluntary (Harris and Maxwell.)

Harris and Maxwell

The Tour de France is an easy choice for where microchipping could help disrupt an already flawed anti-doping program, but I also wanted to understand how the data consumed from a microchip could enhance a legitimate athlete's training regimen. I connected with my friend, Josh Burgess, who is a current MBA Student at Vanderbilt University. He was part of a working group that pitched a business venture based off the LINQ cardiac monitoring device, manufactured by Medtronic. LINQ is an insertable cardiac monitoring device (ICM), that can

monitor heart information for patients with cardiac arrhythmias. It's slightly larger in size than a microchip and is implanted under the chest walls and not the hand. The LINQ device is able to produce more reliable heart data than any smartwatch with an EKG, and it can alert caregivers and family members when arrythmias are occurring (Reveal LINQ.)

Their group used this same type of technology, but targeted Triathletes and Olympians over those with heart conditions. The goal would be for these elite athletes to purchase the device, which they branded "Chypt," and have it implanted the same way as LINQ. The licensing model would then be an annual subscription, and all administration could be delivered through a computer. The group's value prop would be that a device embedded into a person would produce more reliable data about your current health and could give an incremental advantage to an athlete because heart-rate zones become more precise. This product would be publicly available to anyone looking for a competitive edge, but Josh said that almost half of the athletes resisted due to expected ethical barriers like invasion of privacy and the apprehension of not knowing whether your personal data is secure (Burgess.)

While some see human microchipping as an attempt to declutter their life, many will resist this paradigm shift due to the insufficient security on the device itself. A hacker who was attempting to extract sensitive data from a microchip would generally have to be at close range, and often for a set period of time, but an attack could be executed with the right skill set and cyber weaponry. Several years ago, financially motivated hackers could steal your credit card without ever physically touching your wallet. RFID readers can be hidden inside of a backpack or portfolio, and within close range could scan your credit card.

The risk of digital pickpocketing extends past financial opportunities as well. Mike Ehlers, who is a sales engineer at Forcepoint, said RFID and NFC readers can be self-contained

and operated out of a person's back pocket. Modern hotels are issuing RFID room keys instead of the legacy keys with magnetic stripes. The improved experience of opening your hotel room's door is now coming with a price, because a hacker can clone your room key without you ever knowing you've been compromised. This use case goes well beyond identity fraud and surveillance because now the victim could be in physical danger (Ehlers.)

Since 2007, all U.S. passports that get issued contain a small RFID logo on the outside of the passport. It allows customs officials to quickly scan your passport and pull up all contact information including your picture (Lee.) The U.S. State Department claims that configuring passports with RFID tags will help bolster security and dispirit fraud attempts, but a sophisticated attacker could swiftly correlate personal data points to open a line of credit or recreate another passport. The State Department also claims that as long as the passport is closed that it's protected, so investing in a passport jacket or stepping out with a retro fanny-pack could be your last line of defense form having your personal data stolen. The common denominator with these examples is that an attacker would sometimes have to be lingering around you for a while in order to deliver a successful attack. If you're like me, and you like to operate with a suspicious alertness, then you take action, but some may be more passive to this attempt.

One of the leading entrepreneurs for human microchipping in the United States is Patrick McMullan. Patrick and acting CEO, Todd Westby are the co-founders of 32Market, which is a micro market that can be easily inserted into any company's breakroom space. The mission of 32M is to provide a convenient option for employees to purchase snacks and beverages without having to fumble for loose change. The employee can swipe a credit card, use their digital wallet and have their badge ID scanned by an RFID reader which would activate a payroll deduction. I

was surprised during my interview with Patrick to find out what triggered an interest in human microchipping and where he sees the market headed.

According to Patrick, the micro market industry has become more crowded with vendors offering food and drink services that can be unattended 24/7, and they have all standardized on cashless payment options. Being a food retail and tech company, 32Market wanted to pilot an employee microchipping program where they could open office doors, unlock their computers and of course make payments at their own corporate kiosks. In order to stay competitive, they wanted to test use cases that could accelerate workflow and experiment with new concepts for how employees performed basic job tasks.

The adoption rate for this pilot was higher than he expected. Nearly half of the 200 32M employees volunteered for the pilot. I found the statistic surprising given the company is headquartered in Wisconsin, a long way from Silicon Valley. But taking the lean approach to access and payment was not part of Patrick's driving pillars for microchips. Several years ago, his wife was involved in a terrible accident and her injuries were mistreated. The surgery went horribly wrong, and it could have been prevented with the correct health information. Their lives have been meshed with an ongoing malpractice lawsuit ever since and in Patrick's words, "the hospital has put a life sentence of pain into his wife." This inspired his mission for getting human microchips into the public market for healthcare reasons and to allow hospitals and first responders to swiftly diagnose conditions with available PHI data in real-time (McMullan.)

Similar to Peo and Jowan's spinoff company, Patrick started an independent microchip venture called 32Chip. They have active pilots at two major hospitals in Indiana and Wisconsin, and the success criteria extends beyond first responders. They are putting chip detectors into sinks to assure that doctors and nurses are washing hands prior to surgery and are using the chips

to authenticate staff access into a patient's room. This establishes traceability and a root of trust. Patrick continues to evangelize the microchip solution at national privacy events and was profiled on The Daily Show with Trevor Noah last fall. Our conversations became more emotional than I expected. He explained to me how his children would get teased at school, and how religious fanatics would send him emails that microchipping a human being is essentially what John describes in the book of Revelation as "the beast of the earth." His intent has always been to build a company that could help save lives and to be part of something special. I do respect the cause and having the context on what inspired his vision was important for my own conviction.

Three Square Market President, Patrick McMullan

Fitbit recently completed a pilot where researchers analyzed wearable data from over 200,000 users in various states with the objective of determining when the next flu outbreak would occur. They were able to conclude that upticks in heartbeat patterns during sleep cycles is a key indicator that someone is developing flu-like symptoms. This data was confirmed against state flu percentages and could be an important data-stream for the monitoring and treatment of the most common disease in the U.S. (Kim.) Many Americans don't like wearing a watch or anything around their wrist so it's not clear how reliable the data could be without a larger sample set. In the past century there have been two Flu pandemics which ended millions of lives; therefore, microchips could be the silver bullet for being a critical sensor for healthcare but also be invisible to the user.

I don't see human microchipping ever achieving a national consensus due to conflicting viewpoints on privacy vs. security, convenience vs. government paranoia, and those conflicted between choosing to embrace the new digital ecosystem or remaining static in their daily lives until the ethical barriers of technology are fully vetted. There will continue to be a power struggle between the large tech companies harvesting our data, and those who are compulsive about preserving their sovereign identities. If becoming chipped would allow me to take control of my personal data outright and be exempt from any surveillance and behavior tracking, then shouldn't this technology receive positive consideration?

Large tech firms like Google and Facebook stay committed to a business model where targeted advertising is their main revenue stream. This is achieved by consuming as much personal information about their customers as possible. The Department of Homeland Security was created following the terrorist attacks on 9/11, and many advocates for digital privacy are pushing for the FTC to introduce new regulations that can protect our digital experience

(Mullins.) Jowan believes that tech companies could one day launch a program where they give out free devices in exchange for subscribing to their users. Everyone wins in this situation, as long as the person with the shiny new tablet does not care about the privacy ramifications.

With microchips becoming a leading-edge product for access, authentication, payment and healthcare, it's now a very real attack vector for any hacker who's motivated financially or wants to steal an identity for fraud. With so much technology being engineered with "privacy by design" and "secure by default" as their driving pillars, just how protected are the chips being implanted into humans? I personally see the immediate advantages for access, payment, social interaction and just enhancing every sensor I come into contact with. I can now become an upgraded citizen in smart cities that have sustainable environment goals like improving energy and transportation services. Will resisting the migration impede people from connecting to this new digital landscape?

With every conversation I had, the achieved consensus has always been about choice. Every citizen in a democratic nation gets to either participate in technologies that affect them or opt out. Having this social freedom is what helps cultivate our economy and our industries. But the worst-case scenario is when technology starts to turn on you. The microchip use cases that I explored revealed several opportunities where being chipped could improve your overall life. It could provide efficient medical treatment. It could reduce the number of items that you leave the house with. These use cases could ultimately minimize your cyber-attack vector. Most importantly it makes you the sole proprietor to your digital identity. But what happens if your microchip was hacked, and all of your sensitive data can be proliferated in a matter of seconds. I do think that data has become the new oil. It's growing at a rate of 50% year over year, and

within the last two years, more data has been created than the entire previous history of mankind (Marr.)

But when the horse is out of the barn, the damage is already done right? How can users of human microchip technology regain control of their data once it's been shared with millions? It's hard enough to remove pictures of yourself from the internet, and with a microchip in your hand, you are still being digitally tracked and surveilled even after your compromised. Everyone owns a smartphone today and these devices all contain a global unique identifier that lets cell phone towers know who you are. Regardless of whether your device is turned on or off, the device is squawking data to towers and networks. This is essentially what bulk data collection has become, and it's all happening behind the scenes, invisible to the consumer.

As society moves closer to a minimalist approach for data interaction, there needs to be more education on what is on and off, and users must have privacy rights. Putting microchips in humans reduces the clutter, speeds up automation, and could save your life, but all of this comes at the cost of becoming part machine. Every time a microchip user steps out of their front door, they are inadvertently broadcasting RF emissions to the closest data sensor. A tower, a server, an IoT device. These are all proxies for data to be collected and stored forever. But microchip technology could make serious improvements to user privacy and security. Creating an ephemeral mode that required participating systems to delete any collected information is one option. User notifications could be enabled if someone is attempting to scan your device. There could also be configurations that allowed microchips to only function in certain geo locations.

There will always be a debate on whether your privacy is being protected, and perhaps human microchips challenge too many ethical barriers, but the decision to implant a chip into your body will currently be a choice and an accepted risk by that person. Government and

industry will always have a punch/counter-punch relationship with bad actors who are targeting valuable data. It's what keeps professionals like me gainfully employed. At every technology event, you here buzzwords like centralized manageability, seamlessness and automation. Users are becoming accustomed to doing more with less, and a microchip could change the way we do things.

Works Cited

Al-Muaimi, AbdulRahman. "Camel Doping." *ABDULRAHMANALNUAIMI2018.* https://abdulrahmanalnuaimi2018.wordpress.com/2017/08/23/camel-doping/. Accessed 3 Jan 2020.

"Arkangel." *Black Mirror: Second Episode, The Episode of Fourth Series,* written by Charlie Brokker and directed by Jodie Foster, Netflix, 2017.

Bellis, Mary. "Who Invented the Microchip?" *ThoughtCo*, https://www.thoughtco.com/what-is-a-microchip-1991410. Accessed 19 Nov 2019.

Burgess, Josh. "Personal Interview." 3 Jan 2020.

Dzendzel, George. "Personal Interview." 8 Nov 2019.

Ehlers, Mike. "Personal Interview." 5 Jan 2019.

Fawcett, Kirstin. "Microchip." *Wisconsin Software Company Will Microchip Its Employees.* Mental Floss, https://www.mentalfloss.com/article/503055/wisconsin-software-company-will-microchip-its-employees. Accessed 23 Nov 2019.

Goodrich, Michael and Tamassia, Roberto. Introduction to Computer Security. *Pearson New International Edition*, 2014.

Harris, Joe and Maxwell, Steve. "The Outer Line: A New Approach to Anti-Doping." *Capo Velo*, https://capovelo.com/The-Outer-Line-34A-New-Approach-to-Anti-Doping34/. Accessed 4 Jan 2020.

Hering, John. "Personal Interview." 29 Oct 2019.

Kim, Allen. "Your Fitbit could help health officials predict flu outbreaks in real-time." *CNN*, https://www.cnn.com/2020/01/16/health/flu-prediction-fitbit-wellness-trnd/index.html?utm_source=CNN+Five+Things&utm_campaign=fbe5733f0d-

EMAIL_CAMPAIGN_2020_01_17_03_15&utm_medium=email&utm_term=0_6da287d761-fbe5733f0d-105506881. Accessed 17 Jan. 2020.

Lee, Laurie. "The Things You May Not Know about the Microchip in Your Passport." *Swift,* https://www.swiftpassportservices.com/blog/the-things-you-may-not-know-about-the-microchip-in-your-passport/. Accessed 6 Jan 2020.

Marr, Bernard "Big Data: 20 Mind-Boggling Facts Everyone Must Read." *Forbes.* https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#273afdcc17b1. Accessed 12 Jan 2020.

Martin, Nicole "Elon Musk Is Making Mircochips To Link Your Brain to Your Smartphone." *Forbes.* https://www.forbes.com/sites/nicolemartin1/2019/07/17/elon-musk-is-making-microchips-to-link-your-brain-to-your-smartphone/#65227b502412. Accessed 11 Jan 2020.

McMullan, Patrick. "Personal Interview." 18 Sep 2019.

Mullins, Luke. "Do We Need a National Bureau of Privacy." Washingtonian, Dec 2019, p. 16.

Osterlund, Jowan. "Personal Interview." 22 Oct 2019.

Ratna, Sneh. *"*Best use cases of NFC to implement in 2019: Proximity marketing without an app*."* *Beaconstac*, https://blog.beaconstac.com/2019/01/proximity-marketing-without-an-app-best-use-cases-of-nfc-to-implement-in-2019/. Accessed 10 Dec 2019.

"Reveal LINQ insertable cardiac monitor to detect atrial fibrillation after cryptogenic stroke." National Institute for Health and Care Excellence, https://www.nice.org.uk/advice/mib141/chapter/The-technology. Accessed 4 Jan 2020.

Roberti, Mark. *"*What Is an RFID Reader's Maximum Range*?" RFID Journal*. https://www.rfidjournal.com/blogs/experts/entry?10918. Accessed 12 Nov 2019.

Stromberg, Peo. "Personal Interview." 23 Sep 2019.

Taylor, Jordyn. “Can We Microchip Our Kids to Prevent Kidnapping.” *OBSERVER*. https://observer.com/2015/03/can-we-microchip-our-kids-to-prevent-kidnapping/. Accessed 18 Mar 2015.

Three Square Market. “The Microchip – One Year Later, where are they?” *PRLOG*. https://www.prlog.org/12720623-the-microchip-one-year-later-where-are-they.html. Accessed 11 Jan 2020.