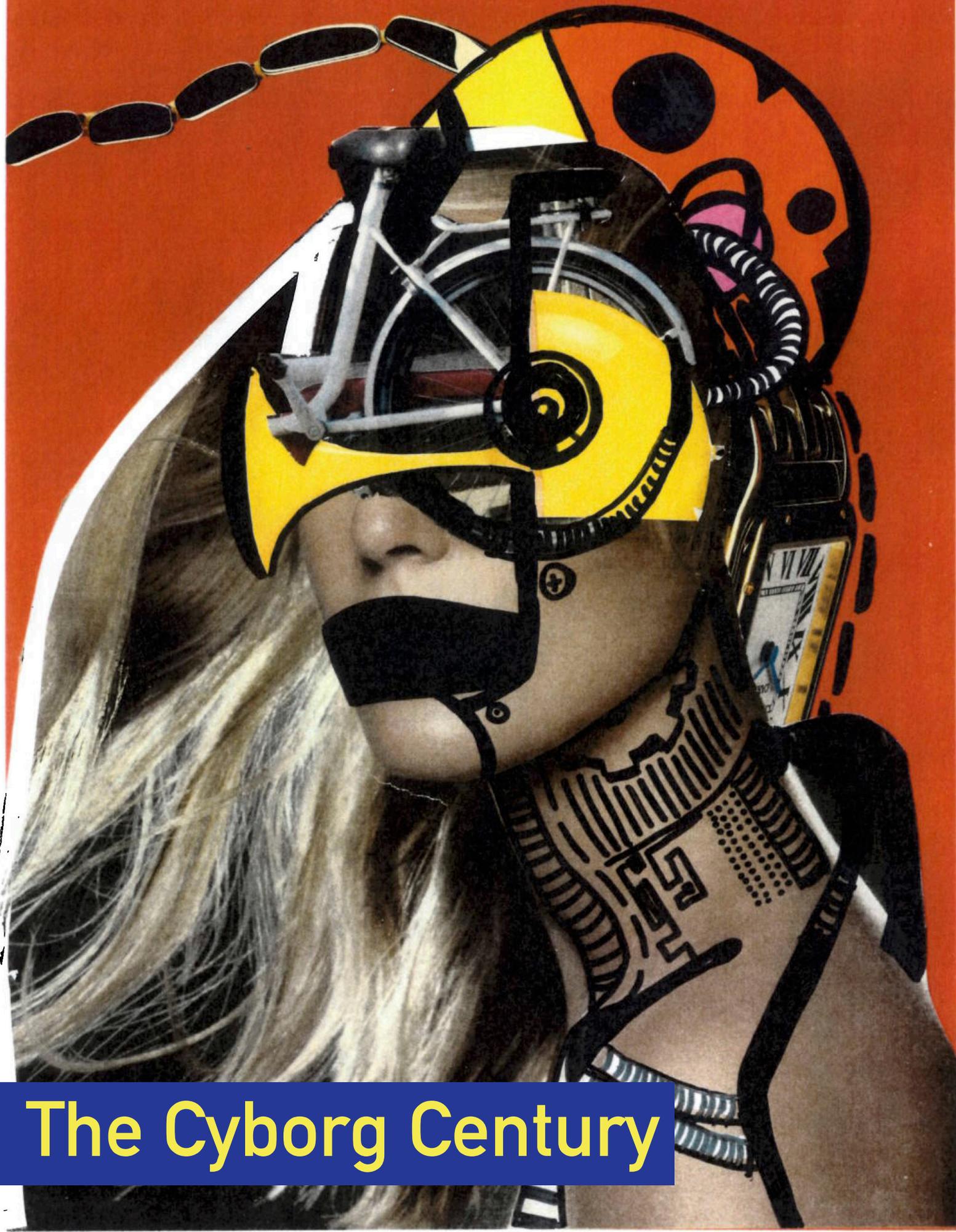


@?TECH.SPECS



The Cyborg Century



The following pages offer a reflection on our cyborg identity within the context of contemporary culture, focusing on how this constructed identity is malleable and capable of being reprogrammed. This reflection in turn raises questions about the role of security in light of an interconnected cybernetic being, that exists within a system, in which the average individual is without much control over their own agency. Instead, we lie helplessly under its grid of control, because

while we might use its language we do not yet fully comprehend it, nor truly understand how it is different to our regular sense of being in and experiencing our world. Therefore, several meditations on philosophical and cultural theory are explored, as pertaining to the area of focus: Our being in and experiencing the world as cyborgs with a cybernetic configuration. Interviews are included as the foundation of the research process, and to aid the reader's understanding by presenting different perspectives from experts in the field. As the theory of aesthetic research demands, the process - which is about collecting, processing, producing, and reflecting on: a topic of particular interest, a sensation, a question, or a concern - is thereby made an integral part of the central theme .

As a female cyborg I inherently view the world from a feminine perspective, undoubtedly coloring my position and influencing my decisions. Within the study of technology and engineering (even the world of business for that matter), and though I always had strong female role models, I did not see a place for myself within this space. For this reason the role of the female is also present within these meditations – though only subtly so; through the discussion of Donna Haraway's essay A Cyborg Manifesto, with the reappropriation of female advertisements and finally a humorous play on the word "Glossary"- Gloss(O)vary – and so reclaiming the concept of man-splaining. In explaining the significance of reclaiming identity amid rapid technological developments and the erosion concerning physical and cognitive boundaries of experience, I have in turn rediscovered my own means for engagement and the process toward reclaiming my constructed cyborg self. The reflection then comes full circle, and with it, a deeper understanding of the central theme. While the field of interest was unimaginably large for a single thesis, the hope is that a reader may, at least, begin to find some insight into the entangled network that we have become embedded in, and be able to conceive of new ways to engage with it, in order to regain a sense of self-efficacy and autonomy in our relationship with this cybernetic jungle.

Recording Interviews
20%

60%

Research, Writing and

2% Coordination & Organization

*The image in the background shows how technology's use was divided between different tasks/activities during the production of this thesis. However, data should never be that easy to piece together.

CONTENT

pg. 3-8

D1g1tal Kn0w H0w

**It's Time to re-program Cyborg Culture
Can You Hack It?**

pg. 10-16

pg. 17+18

Unnecessary Necessities - the Reasoning for
In-Person Interviews

pg. 20-23

Interview with Andrea Mambretti
Part 1

Hacking a Personal Voice Assistant

pg. 25-32

pg. 33-35

Interview with Philip Junker and Nikolas Molyndris

Interview with Cristen Anderson

pg. 37-39

pg. 41-44

Interview with Andrea Mambretti
Part 2

Interview with Umberto Annino

pg. 45-48

pg. 49-52

D1dact1c Tr@nsf3r
- X-pl0ring L1v3d Sp@ce

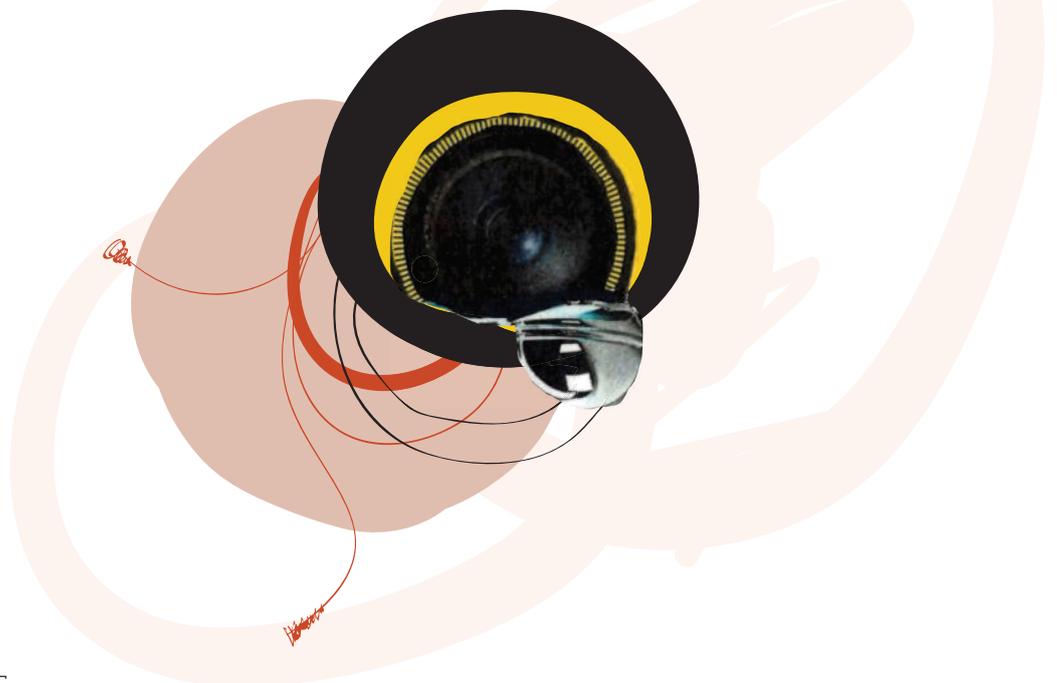
DIGITAL KNOW HOW

Trainspotting

Traveling on the commuter train from Lucerne to Bern, I observe our ritual act of **digital interaction**; engagement with **digital mobile devices**, typically a **smartphone** connected within a **telecommunications overlay network**. Ritual, because to interact with **digital technology** and digital mobile devices has become an increasingly standardized way of being in and making sense of the world. Almost every individual is occupied with either a **laptop** or a smartphone. In fact, a few seem to be using both, their multitasking capacity evenly split between smartphone and laptop, their concentration jumping between the two screens.

In general the only ones who seem to have avoided becoming sucked up into **digital technology's vortex** are 65 years of age or older. Usually travelling as a couple or in small groups, they casually make and eat a picnic, gossip, read the newspaper (on Sundays), or gaze at the view outside as it streams by. Upon closer examination, there appear to be, however, even some among the younger individuals who – as if by some miracle – do not have their noses buried in their laptops. Yet, after closer study, it becomes evident that although the greater part – let's say, 80% – of their attention is absorbed by traditional pastimes, such as reading a book, the remaining 20% of their concentration is taken up with checking their **smartphones**. "But then again, who am I to judge?" I ask myself, as I pull out my own smartphone, an **iPhone**, to change the music, quickly checking if I have received any new **SMS messages**.

Two effects of our digital interactions struck me as odd during these observations. First of all, is that through the increased use of our digital mobile devices, we have become more dependent on conceptual forms of data, forgetting the importance of our concrete bodily experiences. Secondly, is that the way our digital mobile devices function, i.e., the way we use them, serves to blur the distinction between three essential sets of binaries: close/distant, independent/co-dependent, and private/public. I would like to argue that the new, now ambiguous and even paradoxical nature of the relationship of these formerly distinct categories means that we are closer to those on **Instagram** following us – or that we follow – than the people that share with us our daily commute. We have become so effectively productive – posting stories, uploading images, keeping up with the constant stream of news effectively maintaining work and business life while on the go – fulfilling our responsibilities, while at the same time consuming energy resources and our attention, bringing into question our productive use of time.



Body and Mind, Oh My!

It may seem as if our world has become split between the physical reality that our body engages with and the world behind the screen that instead occupies our mind. However, body and mind are not separate entities in a classical Cartesian sense. Our bodily perception is, instead, inextricably entangled with our cognitive conception. The two modes of engaging with our world enhance each other. In this sense, digital technology can be viewed not only as enhancing our cognition and its capacity to process or communicate information, but also as changing the way we perform, the *how* we are being in the world.

Here emphasis is put on the *how* in terms of the *how we know* of epistemology. Although there are considered to be three distinct types of knowledge in epistemology, this essay makes use of two of the three: knowledge-*that* and knowledge-*how*. Knowledge-*that* is the claim that some fact is true. This is also called declarative knowledge. Knowledge-*how* is knowing how to do something, is also called procedural knowledge.

The traditional claim is that making sense of the world requires bringing experience under cognitive concepts. This means that procedural knowledge is subordinate to declarative knowledge. For example, if I say I know that I am holding a cup, it is because I understand the concept of what a cup is and can explain the features that define it as a cup. This view leads to a strong separation between body and mind, positing the body as a mere vessel of receptivity. This notion stems from Kantian Idealism, which explains that our mind possesses conceptual categories which categorize and order our experience into intelligible ideas. Therefore, knowing *how* to do something requires then that I have knowledge of some fact, i.e., I have declarative knowledge in the form of propositions. However, it is possible to think of situations in which such a claim would prove problematic. Take, for example, knowing how to ride a bike. While it might be possible to have a certain set of propositions describing how to successfully ride a bike, like: "I ride a bike by pedaling, by steering right when I want to turn right, by keeping my balance on the seat, etc.", this does not confirm that the person explaining this does in fact know *how* to ride a bike. This is why a more contemporary line of thought recognizes that our body actually plays a large role in our ability to make sense of the world around us and actually possesses its own way of knowing.

Samuel Todes believes that our perceptive experiences dictate what we know. He explains that, "There are two levels of objective experience: the ground floor of perceptually objective experience; and the upper story of imaginatively objective experience, which presupposes for its objectivity (i.e., for its dependability as living quarters) that the ground floor onto which it is built is itself on firm foundation." (Todes 2001, p.100) Without bodily experience – knowledge *how* – there can be no attempt at cognitive comprehension – knowledge *that*. Our conceptual ways of knowing then are what we abstract from these experiences. "We can understand the general but incomplete regularity of our experience only by understanding that it is the experience of a human subject having an entirely governable body..." (Todes 2001, p. 41) The very fact that we are perceptive bodies within space suggests that we have come to know through their experience. However, this is not because we decode a variety of stimuli, but because our body plays an active role in constructing this knowledge. In turn, the mind abstracts experience into declarative thoughts. "To make our world habit-able we need to learn to calibrate our perceptions with how they test out for us as we move about and interact within our physical and social reality." (Strong 2005, pp. 518–519) As we are experiencing and abstracting these experiences, our conceptual mind is creating ideas against which it may later compare subsequent experiences. Psychoanalysis confirms this line of thought through various studies on children's development of agency. Without our ability to sense and perceive our body in space, we would not be able to conclude that we are an individual acting agent within the world.

Illustrating this, Moon Ribas, a self-described **cyborg, cyborg activist** and avant-garde artist notes in an interview with Quartz magazine that "If you modify your perception, in the long term you also modify your brain and your mind." (Quinto 2016) She has had a sensor inserted into her elbow, that allows her to sense all the earthquakes in the world, as it is connected to a live online database tracking seismic activity. "The unity of the world therefore lies in our sense of life, our sense of being an individual self-mover seeking to meet our needs." (Todes 2001, p. 263) While technology might often appear to be a separation of two spaces – the physical and the **digital** – this only appears so because we have two different ways of coming to know our experienced world.



When considering digital mobile devices, it is evident how our physical interaction with their physicality – as **hardware** – opens up new ways of being, e.g., walking while placing a telephone call, holding up the camera to take a selfie of you and your friends etc. Their mobile functionality allows us a wider range of perceptible actions with our physical space. Even the navigation of a digital mobile devices' **operating system** contains modes of physical interaction, for example: when we touch the screen, zoom into an image using two fingers, or swipe up in order to scroll through a **website**. User and interactive design are responsible for all of these features. However, they would have been impossible without the development of **graphical user interfaces (GUIs)** making these **digital system** responses visible. GUIs give the flow of binary numbers a visual layer by abstracting the mathematical foundation that programs are built on into shapes and actions. We perceive this visual layer as an area or space that we can navigate, manipulate, populate, and with which we can interact. Without this visual feedback feature, **computing** would still only exist at isolated universities and research facilities – perhaps at several companies – as high-end powerful calculating machines. This visual framework is what allows technology its '**plug & play**' status. Companies such as Apple have proven again and again just how influential **user-friendly interfaces** and the use of **ergonomic gestures** can be when making technology an intuitive interactive experience.

But other than this, the rest of our interaction with our digital mobile devices is based on a solid framework of declarative knowledge on a conceptual level. Things like digital communication in the form of e-mail or instant messaging are absent of any physical interaction with the person with whom one is communicating. Even video chats only contain a limited amount of perceivable sensory information about the person on the other side of the connection. With mobile devices geographic isolation has been curtailed, if not eliminated, and our time zones blur into another. Bodily procedural know *how* is slowly disappearing from otherwise physical interactions, because they are now occurring in a space in which this physicality is no longer part of the equation.

However, we need both conceptual **and** perceptual knowledge in order to form a complete understanding of our lived experience in the world. This world behind the screen informs in equal parts the actions, thoughts, and relations that are present in a physical sense. Therefore, it is important to question the purpose and use of digital mobile devices. These digital interactions do not inform us on the level of procedural knowledge, so heavy use of these devices might mean that our bodily knowledge shrinks or becomes out of sync with the size of our ever growing conceptual knowledge. Procedural knowledge is essential for our awareness and fullness of being in the world.

The Destabilization of the Binaries - Independence/Co-Dependent, Close/Distant, and Private/Public and Their New Paradoxical Relationships

As I mentioned earlier, the functions and operations of our mobile devices have destabilized the conventional polarity of such binaries as independent/co-dependent, close/distant, and private/public. Beginning with the first of these three pairs, I will consider the changed relationship of independent/co-dependent in relation to an obvious quality of our digital mobile devices, i.e., the fact that they are mobile. This feature allows users to freely move about the world lugging their devices along. While on first thought it might seem that global communication features of the device make it possible for us to become independent of other persons. I can now travel to Amsterdam for vacation, and still be available through instant messaging, calls, or video calls for family and friends that are still in Zurich. However, upon deeper consideration it becomes evident, as stated by Michael Arnold, that: "The [smart]phone does not contribute to independence, and is entirely redundant, if in fact the user is independent of others." (Arnold 2003, p. 244) In other words, the prime function of a digital mobile device is to be able to communicate and stay connected with others as well as to support the user's ability to make social arrangements. Actually, if the aim was to be entirely independent or free of others, then the device would be left at home (as some brave persons even dare to do), and these non-users would just wander off into the woods and return when the sun sets. We are left with a user that is "digitally leashed because [they] are **un-wired**." (Arnold 2003, p. 244)

In terms of the second pair – close/distant –, the physical independence that mobile devices provide, allows persons to be distant physically or even socially, yet reachable at any time. “The connection between physical proximity and social proximity is broken.” (Arnold 2003, p. 245) For example, while I might be sitting on the train with many people around me with whom I choose to not interact, at the same time I communicate over long distances with those physically absent. The irony is that although the user does not want to socially engage with those within physical proximity, he/she is less able to escape the pressing nature of being considered as always available to others. The binary collapses and we are left with a user that is at once close and distant at the same time.

The third and most important paradoxical new relationship of opposites is our sense of privacy when using a digital mobile device. Though a digital mobile device is perhaps owned individually by only one user and has been customized to suit its user’s specifications, a phone call on a digital mobile device is not private when conducted in public space, e.g., the public hearings of private grievances which have become the bane of our everyday life. Moreover, the internal operating system allows the device to be connected to an **overlay network** to access the **internet**, which is required for end-to-end communication. In fact, the greatest paradox is that seemingly private conversations and messages are only possible through the overlay network via the internet, which, in short, means being hooked up into a **public domain**?

The Publicity of Private Experiences

In order to maintain privacy and anonymity, many of these network connections are encrypted end-to-end; meaning that only the two end points of the connection have the key to decrypt the content of the messages. However, communicating with others through the device – generally through various **social media** platforms – itself implies a lack of valuing personal privacy. Suddenly everyone is involved in your everyday life. They can see your posts on **Facebook**, your images on Instagram, and your videos on **Snapchat** or **YouTube**.

But more importantly the degree to which your private communications with individuals remain safe on these platforms depends on a whole combination of variables, for example: the safety and security of the server the network communication, the strength of the hosting website’s encryption, the protocol through which you have connected to the website (See pg. 20 - 23 for interview about all the layers a computer goes through when connecting to a website.) And hackers are constantly looking for ways to break into systems and abuse these systems’ structures so that they can use them to their advantage. At times their trespassing is catastrophic. Just how private is personal information, if hackers are able to access data remotely, i.e., enter the stored files and information on digital mobile device? Further, consider what kinds of extended access they might have once they have hacked into a device. The little pocket assistant that was helping keep track of all your social events, personal information, and much more, suddenly becomes not only a vulnerable keyhole, but also a lucrative bounty of sensitive data. Every digital mobile device, typically smartphones, is connected to an overlay network that uses the internet. The device’s connection to the internet is exactly what can make it possible for hackers to enter the operating system. (See pp. 25– 32 for story about voice assistants and how this can be done without remote access through the internet.) Personal information, as a key component of the private sphere, is valued and believed to be something to protect and maintain. However, with our digital usage it is becoming increasingly difficult to observe the divide between what is private and what is public. Personal data protection laws must be continuously updated in order to keep sensitive aspects of digital identity private. But the GUI’s that make technology more user-friendly have begun to mislead us. We believe our private messages are – private. Our way of understanding the *how* of the digital technology we use works continues to diminish as the features and functions themselves become more complex. This leads to a rift in our understanding of being in the world today.

Leading Knowledge Back to Art

Martin Heidegger was one of the most profound contemporary thinkers to open up thought about technology's essence, which is represented by his 1949 lecture at the Bayerische Akademie der Schönen Künste. His main argument in that our focus on technology's instrumentality – as means to a given end – is misplaced. Instead we should question its Wesen [essence] in order to understand its significance and its inherent purpose in our lives. (Heidegger 1977, p. 22) Heidegger was speaking of the qualities of analogue technologies in an industrial era that were only just beginning to lead to the slow rise of **relay computers**. However, his concern and position are still relevant to discussions today. With the pervasiveness of digital technology in our lives, we ought to be thinking about how we want it to shape our future. For the last seventy years corporations in the industry have been defining the answers in terms of its instrumentality. According to Heidegger, "Technology is a mode of revealing...where aletheia, truth, happens."

In light of our preoccupation with technology, we are revealing aspects of human nature. Take for example the **CGI (computer generated imagery) Artificial Intelligence (AI)** influencer – someone whose online profile is used to advertise brands, and influence public opinion through their followers – lil miquela's Instagram profile. Her account is a collection of photographs of herself in the latest designer clothes while attending the most trendy events. Felix Petty, a journalist for Vice's i-D magazine notes, "it felt most exciting to think of her as a way to question things about ourselves, not machine intelligence," (Petty 2018) suggesting that lil miquela highlights our own behavioral vice of incessant consumption, or traits of addiction and our necessity for dialogical contact and acceptance. We are so concerned about how many things we are doing that are worth posting about, that we forget the insight that can be gained from the experience itself. That what people are saying about us online through likes and retweets is, in fact, not more real or true than what those closest to us believe to be positive traits of our personality when they engage with us over a cup of coffee.

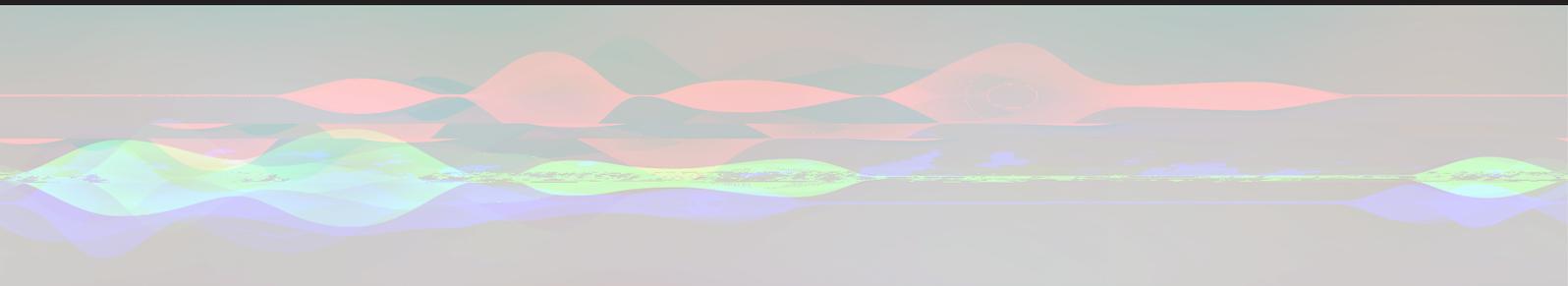
We have become so entrenched in technology's instrumentality to provide the gratification for our formerly physical behaviors, that we fail to recognize, how this satisfaction leads to a dissolution of boundaries and a lack of knowledge how. But the instrumentality of technology is not its end, in the sense of its Wesen [essence]. Instead, "The essence of technology is nothing technological, essential reflection upon technology and decisive confrontation with it must happen in a realm that is, on the one hand, akin to the essence of technology and, on the other, fundamentally different from it. Such a realm is art." (Heidegger 1977, p. 35) as an artist I create, similarly to the way **computer scientists** or engineers build and program, but my process involves reflection not only of the technical aspects and instrumentality of what I have created, but also about myself and my relationship to what I have created. This seems to be what Heidegger was referring to – a position from which critical analysis can be made about "being technological", with the understanding of the word's origin as rooted in the Greek technê as a sense of 'creating', i.e., being creative animals. Within this sense of being, we might come to better understand our condition and situation as experiencing beings in the world, in order to begin altering it, modifying it or **hacking** it to better suit our needs.

When I sit on the train now, listening to music, watching everyone – myself included – looking down at their little pocket assistants, I take a moment to look up and acknowledge the separation between the my modes of knowing, between the text on the screen and the physical sensory stimuli in my environment. I now acknowledge the power, the control, and the right I have in beginning to define my how.



It's Time to Re-program Cyborg Culture.

Can You hack it?



**We are cyborgs –
“creatures simultaneously animal and machine, who populate worlds
ambiguously natural and crafted.”**

- Donna Haraway, 1991

Born in 1944, Donna Haraway is Distinguished Professor Emerita of the History of Consciousness and Feminist Studies Departments at UC Santa Cruz. When Haraway wrote *A Cyborg Manifesto* in 1986 at the age of 42, she had already witnessed the tremendously fast growth and spread of **technology's computing power**. Beginning in the 1940s and up through the 1960s, computers had shifted from being used as scientific calculation machines – spanning the length of large rooms at academic institutions and research facilities – to becoming devices adapted for commercial use. By the early 1980s, this technology had spread to personal use within the home. Though Haraway's main goal in her seminal essay was to address the radical second-wave feminist movement of the 1970s and 1980s that had grown popular in the United States and Europe, she couldn't have known just how prescient of our contemporary culture her “ironic political myth” would become. The **cyborg** is contemporary reality and its very ontology. “We are all chimeras, theorized and fabricated hybrids of machine and organism; in short we are cyborgs.” (Haraway 1991, p.150)

As cyborgs, we blend aspects of our physical bodies and our identities seamlessly into our **digital spaces**; the set of all information in digital form which creates a space that a person can access through a digital interface. (In this sense digital space is lived space, as the set contains both information and the person accessing it.) In turn, our digital spaces inform a significant range of our physical interactions. With the rapid development of **digital technologies**, the machine (both mechanical and digital machines¹) has become integrated with our biology. We have become masters of **cybernetics**, a term first defined by Norbert Wiener to mean “the study of control and communication in the animal and the machine, with the ability to steer both biological and **technological systems digitally**, merging them into each other with every interaction.” (Wiener 1948) It is within this merging that we begin to notice a lack of boundaries and the rise of ambiguity.

Will the Real Cyborg Please **Start Up?**

In short, ambiguity rules contemporary culture as it has become difficult to determine boundaries between the binaries of oppositions such as: human/machine, inorganic/biological, artificial or synthetic/natural, or public/private. While the blurring of these boundaries has led to heated debate and concern on numerous fronts, it has also generated a great deal of freedom. As in the case of ORLAN, an artist, who began a project entitled *La Réincarnation de sainte ORLAN* in 1990. The artwork involved a series of nine plastic surgery operations that altered her appearance, against the common standards of beauty. She states: “My goal was to be different, strong; to sculpt my own body to reinvent the self.” (Jeffries, 2009) In exhibiting control over her own biological features, she wanted to demonstrate the power medical technology might provide us in our striving to become emancipated from previously deterministic biological limits. According to ORLAN, “The real goal was to take off the mask you were born with and reinvent it.” (Sayej 2016)

¹ I include both here, because the development over the last 40-50 years has yielded this shift from mechanical to digital. Without the first, we could not have the second. Though they are different forms of our technological development, they are interwoven into the same timeline.

While breaching such bodily limits between the artificial and natural provide new pathways for invention and modes of discovery, having plastic surgery does not qualify one as cyborg, as here there is no feedback between the organic and the artificial. It is important to mention here again, that according to Wiener, cybernetics as a whole does not simply relate to organic and machine fusion, but to the theories of signaling and communication as a whole. Being cyborg then does not mean to simply augment or enhance the body through wearing prosthetics, as in the case of Oscar Pistorius, who in 2012 was the first athlete to compete in the Olympics wearing running blades. (His participation was grounds for legal rulings against the use of such devices, and their subsequent reversals, as charges were disproven that the running blades gave him an unfair advantage.)

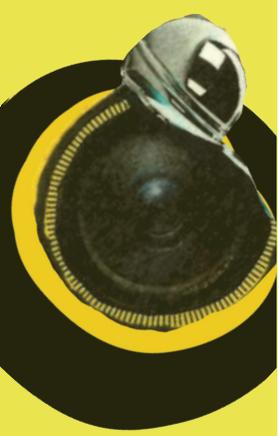
It is never then just the augmentation or enhancement of the biological, being cyborg then always entails signaling and communication as well. Neil Harbisson, an artist and **cyborg activist**, as well as the first legally declared and recognized cyborg under UK law, demonstrates the equivalence of these two modes. Suffering from a rare form of color blindness called

achromatopsia, Harbisson sees the world in shades of grey. In 2004 he had an antenna surgically implanted into his brain so that he can hear colors. The antenna's sensor can receive and transmit information translating sound into color. With his antenna, Harbisson's experience of color is – according to the neuropsychological means – called synesthesia, “in which stimulation of one sense triggers the automatic experience of another.” (Herman 2013) Not only has Harbisson altered and augmented himself biologically, but also his antenna entails signaling and communication. Using his antenna, Harbisson harnesses his cyborg synesthesia to create works of art, vibrant with color. He will often create color portraits of musical compositions, as each color painted corresponds with a musical note. Cyborg status is then not simply achieved by going beyond conventional biological limits, as in the case of those athletes who fuel and train in calculated ways in order to create bodies that are high-performance machines. Instead, as cybernetics in the sense of Wiener's definition suggests, it also had to do with signaling and communication as a whole. So whenever **digital information** is hijacked, i.e., taken up and used to go to a different direction, this is **cybernetic** and can be understood as becoming cyborg.

How a Constructed Identity can fall Prey to its Vices

As already stated earlier, the blurring of separation between such binaries as human/machine, inorganic/biological, or synthetic/natural introduces a world of possibilities. We can use this lack of clarity to push boundaries further and advance formerly static opinions. As a subversive means, Haraway suggests that the myth of the cyborg allows humans to view themselves as constructed. As Wiener confirms, cybernetics involves our ability to steer technological and biological systems digitally. By reframing the individual as a constructed entity, it is entirely possible to alter these systems digitally, and thereby reprogram the notion of identity. The cyborg then can re-generate commonly held beliefs and bring new understanding to binary oppositions. Questioning the *otherness* of being cyborg, we fail to recognize that most of us are not far away from already being cyborg ourselves. We already use our **digital devices** to monitor and analyze biological processes such as breathing, heartbeat, or sleep rhythms to then make decisions or alter our behavior based on deductions made from our gathered results. So, the position Haraway aims to defend is that

by consistently *othering* each other, we miss the opportunity to recognize our similarities and shared interest in – and our shared capability of – re-generating these commonly held beliefs and bringing a new understanding to previously constructed binary oppositions. But Haraway's *Manifesto* is not about “...a dream of a common language, but of a powerful infidel heteroglossia,” which “...means both building and destroying machines, identities, categories, [and] relationships...” (Haraway 1991, p.181) The cyborg is an opportunity to rarify previously held positions of symbolic power. “High-tech culture challenges these dualisms [human/machine, mind/body] in intriguing ways. It is not so clear who makes and who is made in the relation between human and machine. It is not clear what is mind and what is body in machines that resolve into coding practices.” (Haraway 1991, p.177) In this sense the cyborg is **programmable**, our boundaries are ambiguous, and it is up to the individual to construct and reprogram themselves.



In this reprogramming of our identity as cyborg, one must not forget the dangers that face individualized autonomy. When Descartes announced, “I think, therefore I am,” he underscored Western culture’s emerging tendency to consider the mind and body as separate and selfhood as more of a question of mind than body. Unlike Descartes’ doctrine of individualism of the mental, cyborg construction is not about the “West’s... abstract individuation, and ultimate self, untied at last from all dependency.” (Haraway 1991, p.151) Instead, as Haraway notes, “...a cyborg world might [also] be about lived social and bodily realities in which people are not afraid of their joint kinship with animals and machines.” (Haraway 1991, p.154) This speaks of a perspective in which the cyborg must necessarily recognize its undeniable connectivity within a constructed network and its mutual dependency on it.

While Haraway’s prognosis is promising, our collective manner of relating, as demonstrated on **digital platforms** such as **Facebook**, **Instagram**, and **Snapchat**, conveys the potential vice of being cyborg. The cyborg requires data in order to hijack and steer its cybernetic systems. This dependence on information and data is used to feed a corporate capitalist agenda. These digital platforms have begun to exploit the cyborg’s needs, trading its attention as currency. Haraway herself acknowledges that: “From one perspective a cyborg world is about the final imposition of a grid of control on the planet.” (Haraway 1991, p.154), suggesting a darker implication for the cyborg’s reliance on data. Our consumerist culture profits from this need, taking advantage of the West’s tradition of appropriating “...nature as a resource for the production of culture.” (Haraway 1991, p.150) We all need the *latest and greatest* gadgets and to monitor our biological systems in order to control these processes and construct our best self. Ironically in the process, this final grid of control seems to descend over the cyborg itself.

Still today we find that “Our machines are disturbingly lively, and we ourselves frighteningly inert.” (Haraway 1991, p.152) It is simpler to click the *like* button on articles than to engage in debate. Dating **apps** like *tinder* reduce the basis for choices in partnership to the constructed appearance of a person, where pre-selections are made by the swipe of a finger. Our measure of value comes from hard statistical data. We consider the number of *likes*, *clicks*, *shares*, or *re-tweets*, as determining our worth. In fact, China is leading this revolution through Alibaba’s “Sesame Credit” program, which tracks “personal relationships and behavior patterns to help determine lending decisions.” (Mozur 2018) While the cyborg seems to find itself caught under this grid, there is still a positive aspect to our **cyborg identity** that can help us break free from it: the cyborg is, and remains a constructed entity and can, therefore, be **programmed**. And, what can be programmed, can be reprogrammed, and reprogrammed again.

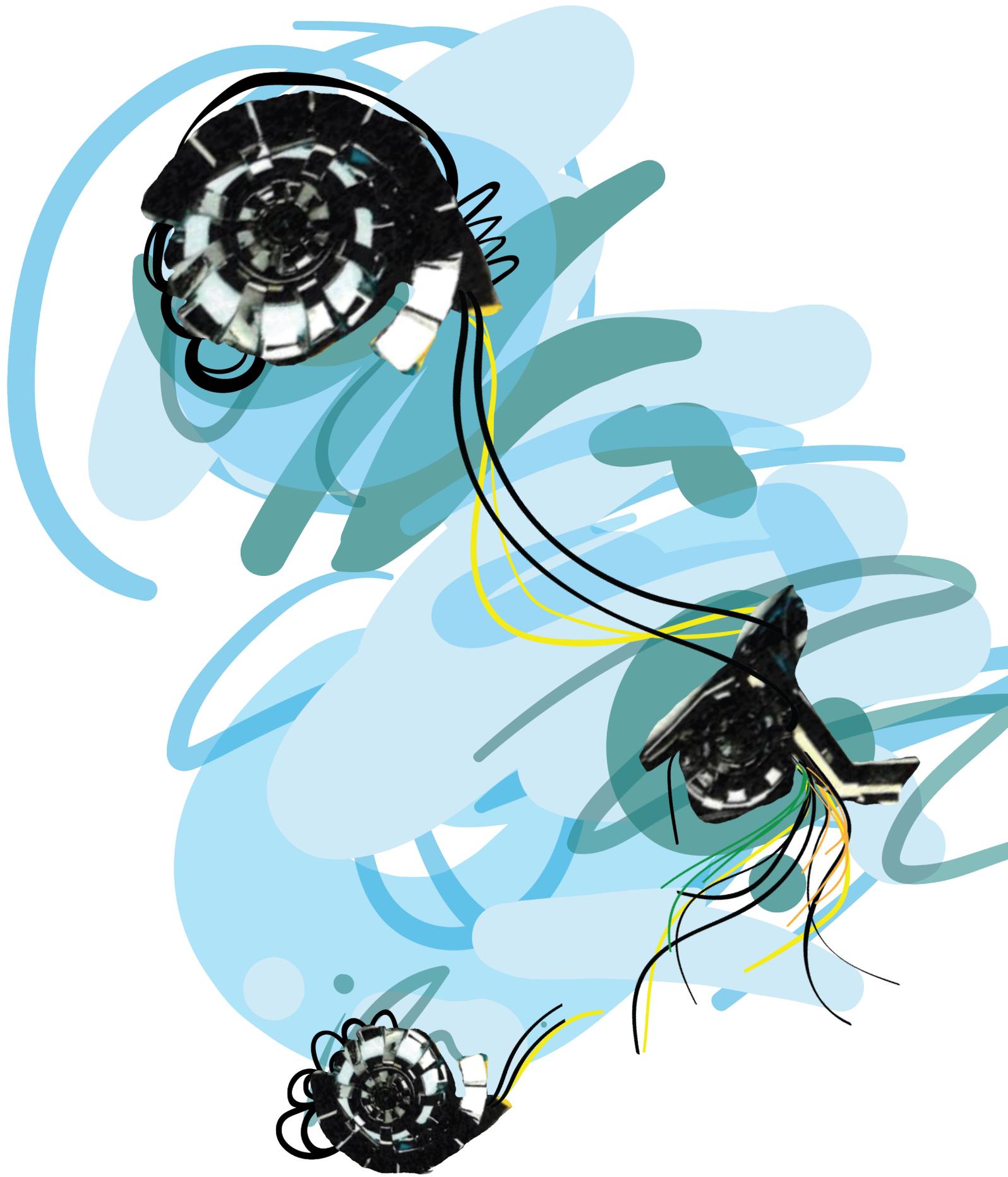
How to Begin Re-programming

Cutting-edge artists today addressing cybernetic and bionic aspects of contemporary culture explore the opportunity to use technology, subverting or reconfiguring its functions in order to shed light on a range of absurd structures, and strange systems. While the aforementioned artist ORLAN changed her facial features in the name of art to point out and re-define aspects of identity and Harbisson celebrates augmenting his limited perception of color via an antenna – by making this condition his artistic praxis – others choose to redefine the mechanical aspects of the cyborg world by interfering with the digital systems upon which it has been constructed. !Mediengruppe Bitnik, for example, finds ways to hack into or subvert systems in order to make its content accessible to the public. In one case, their work *Opera Calling* involved broadcasting more than ninety hours of live opera through the public telephone network of Zurich. (Dörig 2014, p.155) Old mobile phones were modified and turned into listening devices, which were then placed inside Zurich's Opernhaus. By interfering with the systems that surround us, !Mediengruppe Bitnik indirectly questions the individual's role within the network, raising questions about privacy/publicity. In *Opera Calling*, !Mediengruppe Bitnik generates ambiguity by blurring the line between the two and in turn initiates a discussion on the purpose of technology and restrictions set by the system in which we live. By re-contextualizing the way in which individuals have access to a form of culture, !Mediengruppe Bitnik reprogrammed its value.

More directly influenced by Haraway, the Australian artist collective vns Matrix wrote a "Cyberfeminist Manifesto for the 21st Century" in 1991. They too construct a fictional tale, but instead of a programmable identity, they announce that they are the "modern cunt". Instead claiming technology's capability to reprogram the narrative as their artistic method of subversion, by further stating that they are also the "virus of the new world order...terminators of the moral codes...infiltrating disrupting disseminating" (<https://vnsmatrix.net/the-cyberfeminist-manifesto-for-the-21st-century/>) In their artwork *All New Gen* they use technology to produce a video game in which the plot is provocatively re-written to invert misogynistic narratives and satirically refer to pornography. In the game, *cybersluts* infiltrate **cyberspace**, **hacking** into the control and **databanks** of the Big Daddy **Mainframe**.

You, the player, become a component of the matrix and must join forces with the DNA sluts in order to sow the seeds of New World disorder into the databanks and end the rule of phallic power. (www.vnsmatrix.net/all-new-gen/) By appropriating the language of computer technology vns Matrix re-contextualizes masculinist techno-cultural discourses, as a subversion to the authoritative western notions of the self-proclaimed dominant subject; the male. In this work, vns Matrix uses our interaction with digital media as its medium of delivery, whilst simultaneously exploiting aspects of our cultural and social narratives through satire and exaggeration. The system they are reprogramming is the storyline of many video games, with the intention to exhibit re-contextualized and empowered female identities.

Both artist groups – !Mediengruppe Bitnik and vns Matrix – approach their work with a certain sense of playfulness, as they deconstruct binary oppositions. Then through this deconstruction, the opportunity emerges to re-contextualize the cyborg within our digital infrastructure. This is done by hijacking these commonly held cultural and social positions and re-contextualizing the functionality of constructed **cyborg systems**. Their process is "a form of playing around with potential purposes" (pg. 149), which according to Claus Pias is a central characteristic of **hacking**. Moreover, "each new hack simultaneously invents and expands the field of these transgressions." (Pias 2014, pg. 149) Therefore, in exploring the systems through hacking the possibility exists to reclaim our cyborg identity, by re-reprogramming and subverting established systems.





WELCOME TO DOSBOX !!!

Welcome to DOSBox SUN

For a short introduction for new users type: INTRO
For supported shell commands type: HELP

To adjust the emulated CPU speed, use **ctrl-F11** and **ctrl-F12**.
To activate the keymapper **ctrl-F1**.
For more information read the **README** file in the DOSBox directory.
HAVE FUN!
The DOSBox Team <http://www.dosbox.com>

```
Z:\>SET BLASTER=A220 I7 D1 H5 T6
Z:\>mount c /emulator/c
Drive C is mounted as local directory /emulator/c/
Z:\>c:
C:\>CENTIPED.COM
```

Welcome
For a sh
For supp

Welcome to DOSBox SUN
For a short introduction for new users type: **INTRO**
For supported shell commands type: **HELP**
To adjust the emulated CPU speed, use **ctrl-F11** and **ctrl-F12**.
To activate the keymapper **ctrl-F1**.
For more information read the **README** file in the DOSBox directory.
HAVE FUN!
The DOSBox Team <http://www.dosbox.com>

```
Z:\>SET BLASTER=A220 I7 D1 H5 T6
Z:\>mount c /emulator/c
Drive C is mounted as local directory /emulator/c/
Z:\>c:
C:\>Q-WALKER.COM
```



Thus, hacking is an especially promising means for reprogramming the cyborg. Hacking is a subversive behavior that exposes the **technological vulnerabilities** of systems. There is a direct intention to circumvent some sort of feature that was pre-programmed into a system. Hacking is about testing limitations and exploring a system's capabilities. While generally applied with malicious intent, hacking has also always had a humorous side to it. The first **viruses** were visual images of a walking man, caterpillars, or the psychedelic pixilation of your screen, visually notifying you that you had been hacked. **(See page to the Left)** On the other hand, through the act of hacking, it is possible to gain new perspectives on problems and approach a system from alternative angles. This means that there is much to be gained through explorative tampering with the system. By testing the limitations of our networks through manipulation, it is possible to reanimate the cyborg. Awakened by exploring these systems, the cyborg's playful curiosity can pull it out from under the imprisoning grid of control under which it suffers. Through hacking the systems that surround it and gaining new perspectives, the cyborg may come to understand its agency within our ontology of the digital and so reclaim its status as an emancipated entity. The cyborg world requires reprogramming on this level and through hacking the systems we are confined by, it might just be possible to reclaim our digital space.

Whilst Haraway's essay still remains an important feminist perspective, it has now become a bigger critique and question of the picture painted by our use of digital mobile devices and **digital networks**. Though the internet's purpose was to connect the globe, the increase of personal digital mobile devices – generally smartphones – has led simultaneously to the engrossing realization of individual autonomy. This autonomy, in turn, has led to a disruption of previously physical social interactions, replacing them with digital forms of connecting. This has fundamentally changed our mutual collective manner of relating in a way that yields the cyborg more inert than its machines. (Haraway 1991, pg.152) The "cyborg myth is about transgressed boundaries, potent fusions, and dangerous possibilities which progressive people might explore as one part of needed...work," Haraway concludes. (Haraway 1991, p.154) In the end, the cyborg stands for our cultural shift toward virtuality, as an identity whose true existence has not been fully realized; its purpose to "suggest a way out of the maze of dualisms in which we have explained our bodies and our tools to ourselves." (Haraway 1991, p.181) Unfortunately, we cyborgs have not yet managed to pull ourselves out of these binary dualisms. But perhaps through the subversive behavior of hacking these systems, that define our cyborg existence today, we might be able to uncover the paradoxes within their binary oppositions and use this space to reclaim our cyborg identity.



"WE LIVE IN AN AGE WHEN UNNECESSARY THINGS ARE OUR ONLY NECESSITIES."

- Oscar Wilde

Technology has become a pervasive feature of daily life, changing the way we innately experience and exist in the world today. Technology is being created that imitates aspects of human cognition - using concepts from **cybernetics** - giving us the "ability to steer both biological and **technological systems** digitally," (Wiener 1948, pg.11) in order to alter the way we manage our lives. Our **smartphones** are productive organizational tools, that can give us direct feedback on our sleep patterns, or keeping track of physical activity. These technological advancements offer the promise of leading to greater capabilities and efficiency in human live, which, to be fair, it often does.

But, in many ways technology behaves paradoxically, with less than beneficial side effects. Although digital mobile devices may allow users to remain more connected than ever - while still supporting independent mobility - the lack of immediate physicality, highlighted by the user's remote connection via their smartphone, emphasizes their isolation from others. We have become increasingly more busy, while also being constantly available. However, users "...can't be available without taking calls, making arrangements, being booked up and busy." (Arnold 2003, p.248) These situations are ironic, "contradictions that do not resolve into larger wholes...holding incompatible things together because both or all are necessary and true." (Haraway 1991, pg.149) Since I refer to concepts of epistemology, I decided to use the word paradox to identify these ironic situations, as this is more commonly referred to in formal logic. These ironic/paradoxical behaviors in our use of technological devices is what initially captured my attention. I had been observing my own communications through digital media for some time, percolating on the differences between this mode of being and my physical interactions. In our global society, it has become increasingly common place to have friends strewn all over the world in different locations. But, I wasn't sure if my digital communication with another was sufficient enough to truly know who the person on the other side of the screen had become. While this was the starting point for my interest in the often bizarre paradoxes of technologic application, I started noticing that these communications were mostly had while 'on-the-go' through my digital mobile devices. Slowly other strange situations began to capture my attention.

The most bizarre aspect of our technological interactions is our use of voice operated systems. We are all familiar with digital voice assistants like **Siri, Cortana, Ok Google** or **Alexa**. But, these types of systems are starting to find their way into our households. We now have smart-refrigerators, smart-washing machines and even smart-infrared hair removal systems. While the third might not speak to us yet, the other two do. The washing machine will tell you that your laundry is done, while the refrigerator will let you know this morning's news, as you sip on your daily cup of joe. It feels as if a certain intimacy - that remains an integral part of the private household. is being breached. It feels as if in some way our agency is violated, undermining our ability to disconnect from our **digital devices**. (This is something I certainly know that I have fallen victim to and am guilty of.) The concern here is for our lack of autonomy in the digital systems we operate on a daily basis. There is still autonomy in the fact that we use them, and that they provide us with greater methods of obtaining information outside of defined systems such as school. But, the lack of autonomy is in the *how* we use them, as this is generally determined by the companies and developers creating the products we use. The only way to change this would be to learn how to **code**, in order to afford yourself greater self-efficacy in our digital jungle. Initially, my rudimentary knowledge of **coding** and network systems left me feeling vulnerable. In my artistic work I had recently begun to mess around with image data, here I realized that through my immersive explorations I was slowly starting to understand these systems. The insertion of myself was beginning to give me back some form of control - or at least revealing capabilities for their manipulation. I decided that I wanted to continue hacking systems in order to understand their features and limitations. My aim was to regain footing in this **digital space** through a kind of un-learning of what I had previously taken for granted. As E.E. Cummings describes in "The Agony of the Artist": "The Artist is no other that [she] who unlearns what [she] has learned, in order to know [her]self." Maybe this is what my attempt at hacking is really about?

Then Why Conduct In-Person Interviews?

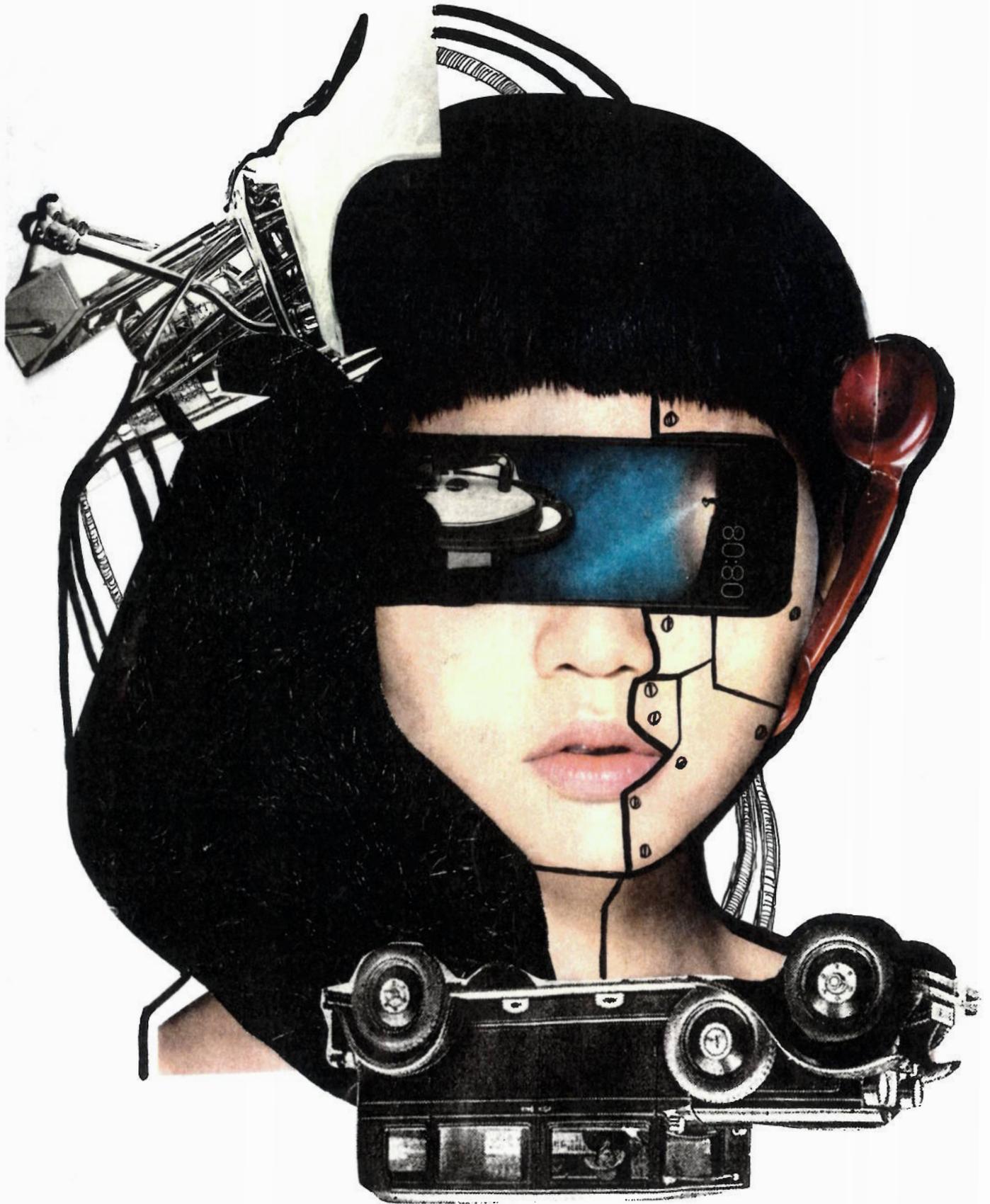
Perusing theory texts and academic writing is a taxing cerebral act that always feels very isolated and static to me. So, I decided to use in-person interviews as a method for my academic research, because I wanted to explore the physicality of my communication with individuals and their knowledge, away from the screens and the digital technologies that otherwise occupy my everyday life. It was also clear that I would be using digital resources to substantiate subsequent research, so I wanted to remain as far away from my digital **interfaces** for as long as possible.

During the in-person interviews my leading questions dictated the general structure and narrative. But with each individual – or individuals – I clearly veered from the initial path, grasping hold of positions and opinions that revealed themselves as carrying greater gravity and weight in the conversation. In each interview I felt it was important to allow the conversation this freedom and to utilize the dialogical dance between individuals, idea, and questions as the driving force of my inquiry. In some ways this reminded me of my endless sessions on the web, in which I traveled down a rabbit hole of endlessly hyperlinked information. However, unlike my one-sided interaction with the web, there was always a second state of being involved in the interviews face-to-face, body next to body. Responding to syntax, vocal intonations, and posture, I was often inspired to engage with more specific aspects of the conversation and discard my script. On several occasions new ideas arose from our mutual dialogue because the interviewees would understand my question with a particular perspective already in mind. But the unpredictable nature of the interview made our mutual discoveries along the way all the more exciting. Once interviewees even began an impromptu conversation with their digital voice assistants. This interaction in particular was interesting, because it revealed our innate curiosity about and desire to play with the systems we use.

With the interviews I tapped into my own personal social network, requesting conversations with acquaintances of mine who I viewed as experts in the field. Here the physicality of the interaction become twofold: not only was I deciding to ground knowledge in a more physical way, but I was also relying on previous physical communications in my physical social network to arrive at these expert sources. In doing this, I discovered the importance that physical proximity can provide in maturing ideas and thoughts. While we rely in many ways on the conceptual power **computing** affords us – relaying data and often superimposing context on it, in order to generate intelligible information – there is something inherently instinctive about conducting conversations and debates through in-person exchange, whereby the senses contribute to the extension and expansion of our knowledge.

The main questions guiding the interviews included:

1. Could you give me a brief summary of how network connections function?
2. How much do you believe the average user understands about these connections and functions?
3. In your own terms briefly defines what a voice assistant is?
4. Explain to the best of your abilities what a voice assistant is capable of doing/executing.
5. In terms of our interaction with technology, where do you see these systems going in the future?
6. Considering our presence on **social media**, is the lack of separation between privacy and publicity even still of concern, i.e., should we care about our privacy?
7. Do you think anything is/can be truly private anymore?



“Computers don’t understand names...”

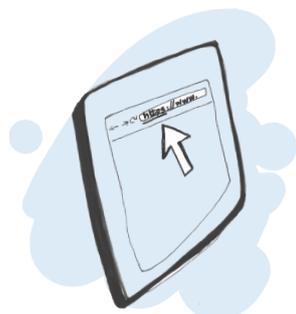
Andrea is in the kitchen kneading pizza dough, enjoying his time away from the screen. He is a young Ph.D. student, and currently a tenant at my mother’s house. At the moment he is working on IBM’s network security at their labs in Rüschlikon. After getting to know Andrea, I explained my thesis to him. This led to many conversations about digital security, and the significance of constantly being connected. In this first part of the interview, I asked Andrea to guide me through the most common network protocols that occur when connecting to the internet, in order to provide a deeper understanding of the process. He begins to explain...

Could you tell me a bit about yourself?

A: Sure! I’m a 28 y-old male (yes male even if my name frequently suggests differently to people) from Italy. My background is in Computer Engineering and I’m currently pursuing a PhD in Information Assurance where I’m specializing in Computer Security. I live in Boston and besides spending my time trying to develop new techniques to defend current computer systems, I play guitar and rock climb a lot!

Could you give me a brief summary of the process that occurs, when I go to a website or try to connect to a network?

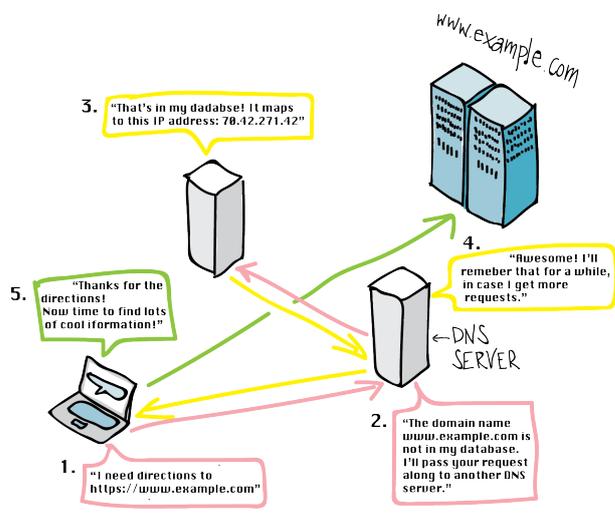
A: Ok, so let’s first take a look at when your computer joins a network. That network can be a cable network, or a wireless network. In both scenarios, generally, your computer requests, or broadcasts, a message based on the **DHCP (dynamic host configuration Protocol)** and requests an **IP address**. Within the IP address it then looks for settings that will allow it to later forward requests to connect to the **internet**. Generally, there is a router, which acts as the access point to the internet, and this access point decides which address this new device—which is trying to connect—is going to receive. Then it can forward the other information, this information can be **DNS** (Domain Name System)



So, what are these DNS?

A: DNS are IP addresses that your device once it is connected receives. Each device gets its own IP, these are the addresses that will contact various sites or ports. It helps computers resolve names, because computers don’t understand names. Even though we navigate using names like, google.com or facebook.com, computers don’t understand those, they understand IP addresses—a combination of **coded** numbers.

So, before connecting to **Facebook**, your computer needs to know where facebook.com is, and which IP address will lead it there. So it’s going to issue a **DNS query**, and once this DNS server receives the query, it then gives you back the IP address of the **website** you want to connect to. So, your computer now knows who to contact, and address to contact, in order to actually access Facebook or Google.



So, going back to the settings that the computer receives, it does not only receive the DNS server addresses, but it also receives the gateways, which is the actual address it has to contact to access the internet.

The DHCP is a clear protocol, because it happens in the local network, and between devices that are nearby. Once you’re connected to the network, and you’ve received the gateway DNS, you then issue a request to connect to google.com. Your computer requests the DNS first, this is the equivalent of the IP address for google.com and then once it gets that information it connects to the website. (See diagram above)

But, there are then several way to connect to the website itself. It really depends on which kind of information you are looking for. Globally, if you connect and navigate a **web server**, you will use a protocol like the **HTTP** or the **HTTPS**. If it’s a HTTPS protocol you’re going to have a connection that is encrypted and is based on certificates. What happens then, is that you have certificates that can be exchanged and keys that are generated for the specific connection you establish. Generally, these days, the sub-protocol that HTTPS uses is **TLS**, which is the standard for that kind of connection.

Is that just a specific algorithmic encryption key—**cryptographic algorithm**?

A: So, generally what happens is that you always have two different algorithms in place for connections. So, all these standards, almost all of them—I don't want to generalize because there are a lot of them, but the ones that I know at least—they always use two kinds of encryptions. The one is a symmetric encryption, and the other is a public and private keys encryption. In the context of public and private encryption the two parties—each side that wants to communicate—they will hold both a private and public key. The public key is of course the one that should be shared, such that the other can use the public key to encrypt messages that are meant for you. But, the person that holds the private key can actually decrypt those messages. This is very secure. The only problem is that the messages that you can encrypt with this kind of algorithm are dependent on the size of the key used, so you cannot encrypt a very long message with those. That is an issue. Because of this, they are also much slower. So, what you do is that you use this algorithm just to set up the connection. What I mean is that you set the foundation to then use a symmetric encryption. In the case of symmetric encryption, you only have one key which is shared between the two parties. This key is used for both encryption and decryption, so if you lose the key, then another person can use the same key to encrypt messages and I would still believe that it's you. If someone tapped the information then they would be able to decrypt what is actually going on between the two devices.

So, this is where the **man in the middle hack** would take place?

A: Yeah, this is would be the man in the middle. (See image below) For symmetric encryption to work, you need to have a moment where you will be able to securely share this shared key. So you use the other one, the private and public keys, to share this other key. Once both of us have this key, then both of us will keep using this key during the session. This is then much faster, because you can encrypt more messages and it works in a different way.



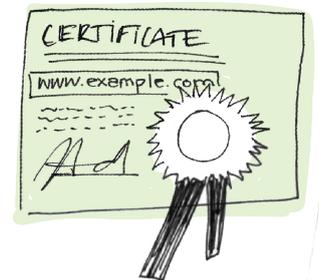
And it's faster because of the length of the key needed to transfer information?

A: No, it's faster because most of these algorithms, that are symmetric, they work per block. So you divide the message in blocks and then each block gets encrypted with this key, in multiple rounds.

The way they have been designed, they generally use specific operations that are very fast.

A sequence of these operations that can process very fast have actually been optimized, so that most of them are directly implemented in **hardware** today. So, for instance, the most famous encryption method that is used is AES, and AES is generally built into the hardware. So, the hardware receives the message and the key directly and gives you back the results super-fast. Here you don't have a size limitation, because it will take much less time for the hardware to process. So, HTTPS uses a combination of these mechanisms to set up a channel that is encrypted and distinct per session. If I connect to you multiple times, then the key is going to change we time we communicate. Each key is per session, to establish our session when I connect to you, I instead use this public and private key. This is all quite generic, there is a lot more complexity within this process, but this is the basic idea.

Ok, so what else—using **certificates**—HTTPS is able to tell if you are connected to the right address. To do this, each side has a certificate and this certificate is generally signed by a certification authority. There are only a few certification authorities in the world, and everybody that wants a certificate has to go to one of them. They hold this root certificate, this root certificate is used to digitally sign each other's certificate during a session. Whenever you request a new certificate, you go to one of these people and you have to prove that you own the domain name "google.com", for example.

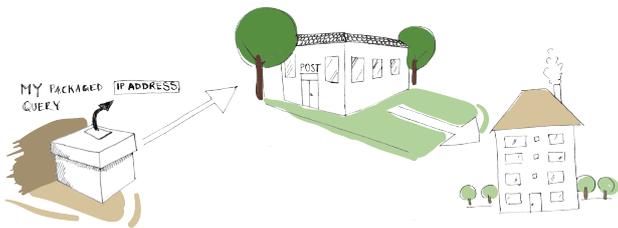


Once you prove this to them, they will sign the certificate saying "google.com" belongs to you. Once they give you the certificate you can set up your server, that will then always use that specific certificate. The server then sends you this certificate and you can verify that it is digitally signed by the certification authority route certificate. By verifying that, you can be sure, through the third party certification authority that you are actually "google.com". So, if I wanted to set up a server that would trick you into connecting with a fake google.com server and not Google's official one (**man in the middle hack** - image to the left), I will not be able to provide you a valid certificate for this fake google.com, because I cannot go to the certification authority and get a new certificate for the same domain. Your browser will detect this, and it will provide you with visual feedback saying that there is something wrong with the connection. That's another layer of security with the HTTPS protocol. Meanwhile the connection protocol—the single session on the wire—is protected by **TLS**.

So while you're connected through this HTTPS protocol, the session maintained by the TLS?

A: No matter what type of communication you send, it will go through a bunch of layers. Each one of these layers is in charge of a preamble header for the package you will send. On the other side the same series of layers will be read in the opposite order they were packaged together as. So, each one of these layers is going to read parts of this information from the package. HTTPS is the one on the top, then there is TLS and then there is **TCP/UDP** and then there is the IP protocol. After that there is the link layer protocol, and then comes the wire. Each protocol layer checks for a specific action/command.

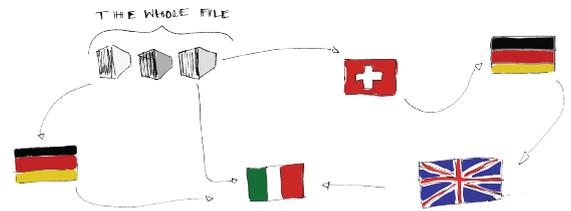
So for instance the link layer is the one that connects, rather makes sure that this package is going to arrive between you and the access point. It will contain the information about you and the access point. Then when it reaches the access point, the access point is going to communicate this package to someone else. That link layer is going to lose your **MAC** (media access control) address and relay your access point as the initial source of the message and look for this other device that you are trying to reach as a destination. So, its verifying that the one to one connection is valid. Then you have the IP which is on top of this link layer. It is going to have the information about the source IP (you) and as a destination, who you want to reach. So this makes sure that whoever is encountering your package knows where you want to send it to. So whoever you encounter in the network is going to see the destination and just keep delivering it to the next server until it arrives at the destination IP. This step is kind of like our normal addresses. You send some mail, and this mail has my address in Italy. Whoever is holding it knows that if this package should arrive in Italy, then it should be sent to the next post office in the direction of Italy. My mail is not going to suddenly go toward Germany or something like that.



So the whole concept in the one to one is that the MAC address is between post offices—these individual steps between post offices—and the IP address is the equivalent to the actual home address. So, they will just know, that to deliver to this IP—or to this address—you need to go in that direction.

Then on top of that is **TCP** or **UDP**, which are protocols that manage the communication in the sense of, that they make sure every package arrives. What happens is that if you have a huge piece of data you want to send, this data cannot be sent all together. So it will be put in chunks, and each chunk is going to be a separate package. What happens is that when you start to send them, it is possible that based on the congestion

of the network, some of the packages will have to take a different path to reach your destination. For instance, part of my information, if I want to connect to Italy, might actually go to the UK and then down to Italy, because that is the fastest route in that moment. Whilst others might just go down straight from Switzerland, and yet others might first go through Germany, and so you need a way to put all the pieces back together. To do this you need to know the order, because you might receive the last package before the first one. TCP thinks about this and manages the process. Meanwhile UDP, which is another protocol in the same layer, won't think about how to put them back into order if they arrive out of order, it will just drop them. UDP doesn't care. TCP notices if some packages get lost and after a certain time will request that specific package, and UDP wouldn't do this. So, UDP is used for example when streaming. Because when streaming, you receive a constant data flow, when you lose a frame, well, who cares, it's not important.



Meanwhile if you're transferring your pictures to the cloud, you want them to arrive in one piece, because you don't want pieces of your images to be missing. There are also other protocols, but these are the two famous ones that our implemented most frequently in our devices.

Next is the **application** layer which is like the protocol that the applications use to communicate with each other, and here there are hundreds of them. I can write my own, for example. The web decided to create the HTTP, and so the web is based on HTTP. If you want to be supported by the web, then you write **code** in HTTP. All your browsers already talk HTTP, so in order to communicate easily with them you write in HTTP. HTTPs then is just an extension of HTTP. So they use the first stage of the IP but then also the MAC protocol and key exchange systems to securely relay information within a session.

I remember now, watching a video explaining the difference between the UDP and the TCP protocols.

A: Yeah, it is very important to understand this on a very generic level. If you program on an application that uses the network, you need to understand concepts behind what is going on when you send something through the application to other devices. The full understanding is not required, but at least the general concept, because sometimes your application will not work for a specific reason and this might be due to one of these processes.

So a bit of knowledge of this is very helpful, if you want to program.

Great, that brings me to the next question: How much do you believe the average user actually understands about these network functions?

A: Zero. The normal user that uses their phone or laptop—zero. Because, they are not required to. There would be a usability problem if we asked the normal user to know all of these things. The whole concept of computers is built on abstracting. Everything in computers is an abstraction of something else. So each layer is an abstraction of the layer beneath it, and the user just sees what is on top. This is just an abstraction of what the algorithms do.

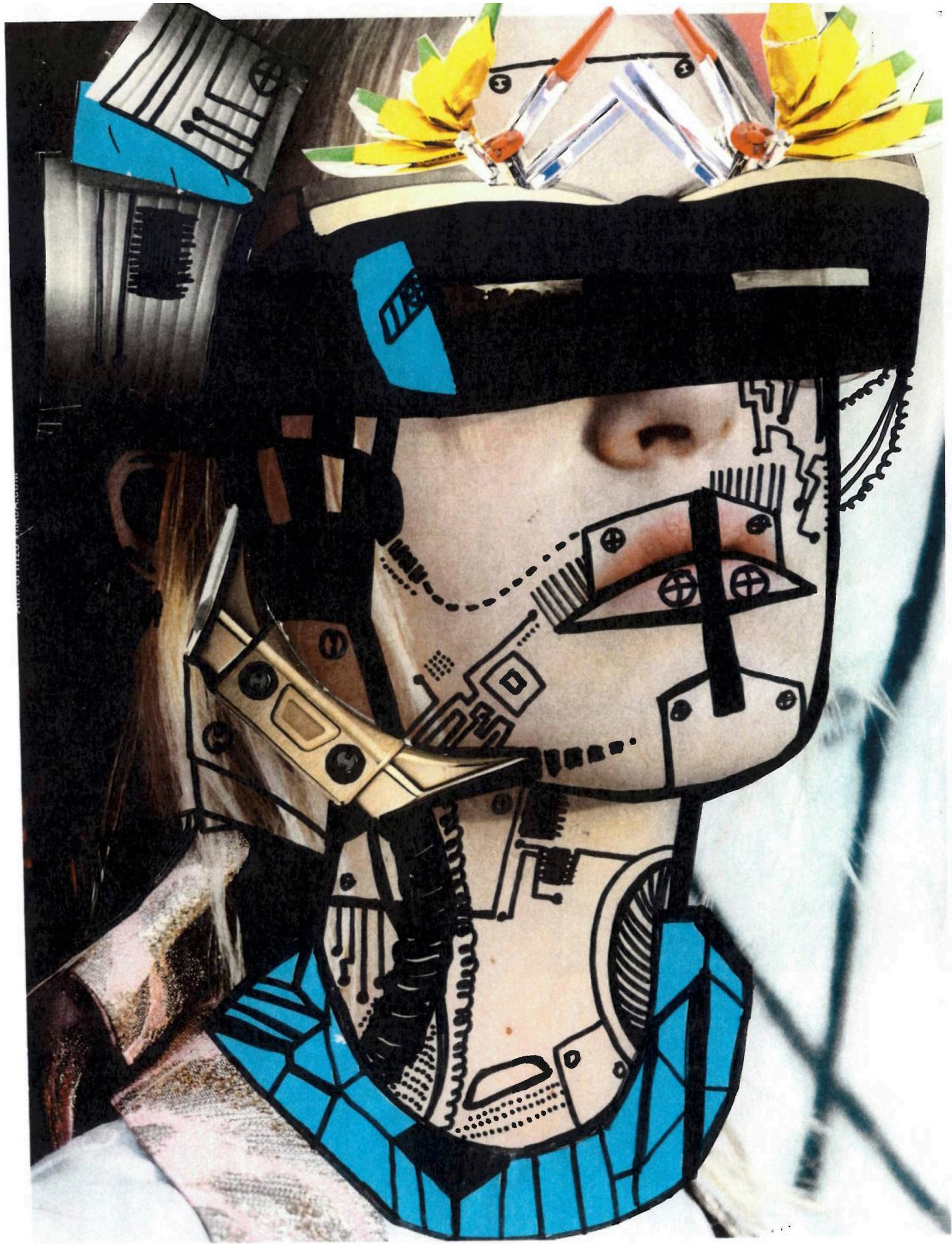
There is abstraction even on the level of the actual physical electronic processes behind the functionality of the device, that then connect the right functions.

A: Exactly, I mean I use **CPU's** all the time. But, I have no idea how the transistor works inside the CPU. I have the abstraction of the fact that this bunch of transistors is used to bind together a bunch of binary numbers—I know that—but I do not know how they are shaped. But, if you design hardware, you should know. The end user is not required to know all of this.

Right. You've just touched on my next question here. To what extent do you believe it is or isn't important for the normal user to know something about these connections and network paths?

A: I mean of course if you know a bit of this it is really helpful, in the sense that you don't have to go to the tech guy for the problems you may encounter. This kind of autonomy can be really helpful and save money or avoid delays when something happens. Or at least you would know how to trace back the issue and figure out which layer is encountering a problem. But the question is: how many people have the time to spend on this? Because it requires a lot of time, right. So, it's a tradeoff, the normal user wants **plug and play** things. In fact, computers became widely used when they developed into plug and play machines. I mean for example the system interface, this isn't required for the computer, but it helps people see elements of the process. This was a big change that really enabled personal computing.—

[See **page 41** for the second part of the interview]



Hacking a Personal Voice Assistant

```
for (var "Siri,I'mhungry," =text(content.a);
```

```
if(Siri has become a friend and helpful companion to many. Apple's digital voice assistant is a computer-engineered program that parses-analyses-syntax of spoken words from natural language into defined electronic actions. In short, "Siri understands your voice and places what you say in context with the apps that it works with." (Sadun & Sande 2014, pg.1) If you tell Siri, "Siri, I'm hungry," she will humorously respond with: "I understand eating is the cure for that." This response is then promptly followed with a web search for restaurants and cafes nearby within Apple's native-map-application. After listing your choices, Siri will ask you if you would like her to call the first location on the list or if you would prefer she give you the directions to the address. Depending on your response, Siri will then dial the number or begin directing you to your desired location.);
```

```
while(Siri may to some degree be considered artificial intelligence (AI), a term originally coined by John McCarthy in 1956 to describe "the science and engineering of making intelligent machines, especially intelligent computer programs."(McCarthy 2007, pg.2) AI is an area within computer programming that has developed drastically since the term was first coined due to the increase in processing power available in computing. While Siri might not cover all areas and applications of AI, she is capable of speech recognition and understanding natural language to a relatively high degree of proficiency. However, the software behind this digital voice assistant is limited to the structure of its code. So Siri cannot truly think for herself because she can only learn from and respond to known or familiar variables in an environment that have been accounted for in the code.);
```

```
while(The software that steers most digital voice assistants - and, of course, Siri's responses - is generally built on a complex structure of code called a neural network. Neural networks are structures that attempt to imitate the decision pathways of our own cognitive logic and are part of a larger field of study called machine learning. Machine learning, as the name indicates, is about creating systems and software that can learn from data and progressively improve - or construct new - features of the system. The study of machine learning explores the construction of algorithms that can learn and make accurate predictions from large sets of data, leaning heavily on various research stemming from cybernetics.);
```

```
while(Strangely enough, neural networks are not a new concept. In fact, the term was coined even earlier than John McCarthy's definition of AI. In 1943 Paul Otlet, a Belgian entrepreneur, conceived of neural networks at a time when the idea of having a responsive system that could parse spoken word - or any complex data for that matter - into intelligent electronic actions was still pure fiction.
```

Today neural networks are quickly becoming the new standard in the field of machine learning, the aim being to create **digital devices** that no longer require a **feature engineer** to dictate the software's parameters by **hard-coding** them into the system. Instead, the definition of the neural net's architecture enables the software to set the most efficient and effective parameters for itself depending on the task it should perform. At the moment, these networks are difficult to comprehend. Even **computer scientists** researching machine learning have a hard time understanding which part of their neural networks recognizes which characteristics of the data. This makes it extremely difficult for engineers to adjust them accordingly and use them with more targeted intentions. Two of the most challenging aspects of this are: getting enough valuable data to train the system, and defining an structure for optimal network efficiency. The end goal is to streamline the processing of data and **parsing** of information: to have systems in place that can help users filter out and key the features of these large **data sets** of which users are quickly losing an overview.);

```
else( According to computer scientists, the hope is that, in the future, these neural nets would be processed and stored locally in the device's hardware. This would then allow the voice assistant's process of learning to be more individually customizable so that they respond directly to all of the user's interactions, and adjust themselves accordingly. A system like Siri would then become the embodiment of the various digital assistants we have come to know through pop-culture, such as KITT in the TV series Knight Rider or Tony Stark's digital assistant JARVIS. Perhaps when you tell Siri then that you are hungry, she would instead know enough about your recent habits and interactions to suggest that new trendy Sushi bar you walked past just the other day, or had been talking about with your friends. If this is starting to sound like science fiction, well, at least at the moment, it still is.);
```

```
for (var Sir, We've Got a Location! =text(content.b);
```

```
if( Though we have not yet managed to recreate the digital assistants we've read about in comics or seen in pop-culture films, our current systems are quite good at creating the illusion of intelligence. Often the code is still very statically written, requiring feature engineers to train the system with large data sets over time. This means that in order to train Siri, Apple requires user data. To do this, "Siri uses information from your iPhone. Data from your contacts, music library, calendar, and reminders [to] fuel its recognition vocabulary." (Sadun & Sande 2014, p.5). How this information is obtained, however, remains a company secret. Companies such as, Apple, Google, and Amazon, involved in the development of digital voice assistants, ensure their customers that their personal information, i.e., their privacy, is protected through the encryption of data using a method called differential privacy. Differential privacy aggregates data collected over time. While data is collected in order to improve products and train systems, the specific user remains anonymous.(Zhu 2018) However, "Your Siri account remains on Apple's servers, and your recognition rates improve over time." (Sadun & Sande 2014, p.11) So, it is unclear as to whether Apple really does apply differential privacy in a completely anonymous way as google is obliged to do.);
```

```
else if(Not only is this trade secret a matter of economic advantage over the competition or even over customers, but it is also a feature of any company's identity. Depending on their business model, these companies will have different interests in gathering different forms of data, which might involve different methods of obtaining it. It is then not only about what information is obtained but also about how and why. A notion confirmed by Umberto Annino, president of the Information Security Society of Switzerland (ISSS). Aninno suggests that a company like Amazon - who were amongst the first to use digital customer profiling - for example, has an interest in making sure that the aggregated information from an Alexa, a home listening device, is available to the company. If information can somehow be aggregated from these devices, Amazon can peer into our private lives in this way, learning more about their customer's purchasing needs and trends. (Annino 2018) This raises concerns with regards to questions about topics such as the difference between public vs. private bodies, and their interest in personal privacy and the legal attempts to protect it.);
```

```
while(While it might be the case that there are many recent efforts to protect personal information, companies must keep records for "up to five years" (Mambretti 2018) due to compliancy regulations. This fact is supported by stories and cases in which the government or police have subpoenaed an iPhone or a home listening device like Alexa in order to gain access to the recorded information. (McLaughlin 2017) However, the real issue with the protection of personal information does not necessarily always involve the company and its servers. While these cases highlight the issue of protecting personal information in our digitally networked environment, large companies often have the manpower to invest in efforts to protect privacy and strengthen security. These companies are also held accountable to many laws and restrictions, in an effort to maintain an agreed upon standard of handling sensitive information. But, our smartphones are not only constantly linked to remote servers, they are also bound to our own physical mode of being in the world. As we travel and commute, our digital mobile devices are right there with us. Therefore, the real issue becomes this proximity between us and our digital mobile devices.);
```

```
while(With our devices on us at all times, we have become trackable entities. Our smartphones behave paradoxically: though we are more independent as we travel, this is contingent on our reachability, which necessitates that our smartphones be on us at all times. The science fiction fantasy of subcutaneous tracking implants in humans is has been rendered unnecessary thanks to the simple presence of our digital mobile devices. Applications (apps) like Snapchat or Instagram have an insidiously eerie way of making a fun occasion of the fact that our mobile devices are being tracked. And, indeed, this is not only fun, it is something that surprisingly arouses our indifference. Snapchat - which allows sending temporary pictures and chats to friends or acquaintances - is a popular app amongst teens.
```

The latest version of Snapchat contains a map, which is difficult to locate as it requires a specific sequence of swipes and clicks that a user must first navigate through before finally finding. The map shows where friends (who have an account on the app) are in real time. While other applications like “Find My Friends” require that the two users agree to the mutual disclosure of their locations, Snapchat instead makes this an active function within its default settings. Without knowing that the pre-setting makes this function active, as well as that it can be turned off, the user’s location is visible to everyone she or he is connected to or following with the program. In fact, it is estimated that about 75% - 90% of smartphone users in the U.S. have their location services turned on. (Anderson 2016) This raises the question as to whether these cool, hip, useful, and efficient apps are worth the potential risks to and dangers of infringements of personal information protection regulations that may arise through their use? But, more importantly: are we even aware of what these infringements might be?);

else(It could be argued that there are ways to interact with these technologies, systems, and software in a more mindful way so that personal information remains protected. Moreover, it could also be claimed that the average user is quite aware of the risks and dangers of using such software because the users themselves employ their features (such as location tracking). But certainly, a counter-argument could be made that there is a problem of a nearly immeasurable span between levels of complexity of use, i.e., most software appears easy, against its complex functions. Further, not only does software involve complex functions, but there is also the complexity of the many levels of the overlying networks - of which our mobile devices are a part of - and this is something that “users are not expected to know about...” (Mambretti 2018) On the one hand, to be a mindful user means to understand how and where to look for these levels of functions. On the other hand, without higher and continuing education in computer science and [programming](#), the gap between complexity of use and complexity of function continues to broaden. A recent court ruling underscores this discrepancy whereby [Facebook](#)’s default privacy settings and use of personal data were ruled illegal in Germany (Hern 2018). The court determined that aspects of Facebook’s manner and extent of obtaining personal information were incomprehensible to the user and therefore an infringement of the protection of personal information regulations. As a result of this ruling, Facebook is now making an effort to significantly change their privacy features so that the average user can easily operate and alter these settings. But even if the protection of personal information on social network platforms is strengthened and users have secured themselves mindfully against various, undesired tracking systems - all of which are encrypted and stored on remote servers - there are still aspects of the device’s physical hardware that can be covertly turned against the user in malicious ways. The exploitation of a digital mobile device’s vulnerabilities in this way is known as [hacking](#).);

```
for (var "The Hackers Dirty Duty" =text(content.c) ;
```

```
while(Hacking is often seen as an infringement of personal information  
protection regulations and, when detected and traced to the perpetrator,  
is regarded as illegal activity. But it can also be maintained that a  
hacker never intends to break the rules of the system he/she encounters.  
Instead, hacking can be considered to be about testing a system's  
limits. For example, Claus Pias, a German media theorist, defines hacking  
as "playing around and testing, combined with a certain lack of respect  
for regulations, system administrators, or contexts of use." (Pias 2014,  
p.147) In essence, hacking involves taking parts out of their original  
context and re-coding them. The process often reveals aspects of a  
systems functionality or dysfunctionality that have not yet been  
considered. In fact, most companies in the digital technology sector have  
designated teams whose task is to stress their systems.  
These teams intentionally hack the company in order to determine  
where potential vulnerabilities may lie, and they work on developing  
solutions to the problem. This exploration and testing is not only  
preventative but supports advancement: "Hacking [leads] in the area of  
knowledge about the new functionality and (im)materiality of devic-  
es themselves-it [is] a form of playing around with potential purpose."  
(Pias 2014, p.148) We can see this in the case of the blue box.  
In 1960 Bell Technical Labs released two papers, both outlined new  
signaling systems for the use of single-frequencies in telephone  
network communications; making telephone network communications more  
efficient. (Weaver & Newell, 1954) These single-frequency dial-ups used  
frequencies to start or end calls and transmit the called number on  
long-distance telephone connections. In order to circumvent the toll  
charges on these connections, collected by the telephone companies,  
engineers began hacking the system - a process known as phreaking.  
The discovery was made was that these frequencies could be  
imitated through whistle tones. In fact, the American breakfast cereal  
Cap'n Crunch included, as a free gift, a whistle that just happened to  
generate a 2600Hz tone - one of the frequencies that was often used.  
In using the Cap' Crunch whistle, a new functionality for its use had  
been discovered - to route phone calls without paying international  
charges. (Rosenbaum 1971)) ;
```

```
if(Hacking then is about uncovering aspects of a system's vulnerability  
and using this knowledge in basically two contrary ways: on the one  
hand, the vulnerability can be exploited in a malicious attack, or,  
on the other hand, the knowledge can be used as a springboard for  
new developments to amend or diminish vulnerable features. In this  
sense, the hacker "oscillates between subversion and stabilization."  
(Pias 2014, p.152)) ;
```



```
for (var "What We Can't Hear, Won't Hurt Us" = text(content.d) ;
```

```
while(After all internal settings have been mindfully attended to, what aspects of a smartphone's hardware might still infringe upon the protection of personal information? Returning to Siri, as described by Sadun & Sande, "[Originally, users] noticed that even when they had a passcode set on the lock screen, someone could pick up their device and issue commands to Siri...Unauthorized users [could] do everything from writing an email or send a text message to maliciously change calendar appointments." (Sadun & Sande 2014, p.98) Second-party access to communication with Siri is indeed a vulnerable aspect of the respective device.);
```

```
if(A group of researchers at China's Zhejiang University discovered that it was possible to unlock Siri using inaudible ultrasonic voice commands. They were able to successfully ask Siri to place calls without any audible sound since the MEMS microphone is actually sensitive enough to detect high-frequency sound waves in the ultrasonic spectrum, which is generally any frequency between 25-30kHz. (Zhang et al., 2017) The implication of the microphone's feature to detect such frequencies suggests that someone could remotely initiate any process that a digital voice assistant is capable of executing within the smartphone's operating system without the user's knowledge or consent. The success of this experiment was confirmed by another research paper published at Cornell University. Both experiments proved that such an attack could be initiated at a range of three meters: All it would take is an algorithm to modulate the human voice into this ultrasonic frequency range. Both teams even took into account the possible barrier of the digital voice assistant being trained to only respond to a specific user's voice. They then suggested ways that this additional security measure could be bypassed, by stringing together different syllables of the user's recorded voice. (Of course, the voice would somehow have to be recorded, but methods to accomplish this, e.g., a telephone survey, are easily conceivable.);
```

```
while(Subsequent research led by Efthimios Alepis and Constantinos Patsakis at the University of Piraeus in Greece demonstrated just how much sensitive information could be leaked by such an attack. In their paper entitled Monkey Says, Monkey Does: Security and Privacy of Voice Assistants, they identified a network of dangerous permissions - actions that can be performed using functions of the operating system only with an authenticated user (generally the owner of the smartphone) - showing how various system commands were linked to one another. In their study they considered a variety of digital mobile devices, discovering that those running Android operating systems proved to be the most vulnerable, the reason being that the applications in this system are all automatically linked to greater streamline user customization.);
```

```
else if(After reading these studies, and being thoroughly freaked out by
their implications, I decided to play around with Siri. Immediately I
noticed that unless I trained her to my voice or physically held down
the home button, it was not possible for me to interact with my voice
assistant. While this assured my conscience that I would not be hack-
able through an ultrasonic attack, I still became worried about my
digital footprint. After all, I tend to store all of my online
passwords to website accounts on Google's keychain. Google's keychain
can be logged into through your Google account, and by clicking on
the eye icon next to each website in the list, I can see my password
for that site. Therefore, if someone hacked my Google account they
could easily gain access to all my sensitive data. But, then again
clearing this keychain means that I would have to remember the vari-
ety of passwords I rotate for each website, as each time I would be
prompted to log in anew. While this example shows that privacy needs
to become a more intuitive process built into the systems we use, it
is ironic that we should be more concerned about those devices which
are more intuitive and have entered our personal space, and house-
holds. These devices have the ability to listen in on everything said
at home. After reflecting back on the studies, it did not surprise me
that Alexa was the most vulnerable device. Amazon has built its
business on understanding consumer behavior, by gaining insight into
any keywords or phrases spoken at home, they become privy to a whole
different dimension of our information.);
```

```
else(At that moment I decided I would recreate the hacks conducted
by these universities, and I would try to secure a footing in
the paradox of my independent dependency on digital mobile de-
vices. If I was going try to understand these systems that I've
become entwined with, then I was going to have to begin hijack-
ing their original purposes in a playful and explorative way.
As an artist, the excitement of new territory - of the unknown
- was exhilarating. Reclaiming my autonomy through this process
of exploration has proven to be just the beginning of what I
hope will become a long journey of discovery.);
```

“Ok Google, you are useless!”

St.Gallen, March 9th, 2018

It is a slow moving, but beautifully mild Swiss afternoon. Nikolas, Philip and I sit on a sofa in Nik's apartment in St. Gallen. I met these two students at an event last December, hosted by the 'Rockethub', the ETH's entrepreneur club. We quickly bonded over some Glühwein and beer, while our conversation wove through discussions about cryptocurrencies to artificial intelligence, and into philosophy. Since then, we meet regularly to discuss our current musings, the latest technological debates and life. I have chosen them for this interview to offer a more casual perspective on Voice Assistants and digital privacy. Though both are articulate in matters of technology and pursuing their Master degrees, our humble conversation is nevertheless one many might encounter on a daily basis. They look at me expectantly; this format feels foreign to us.

N: Nikolas Molyndris

P: Philip Junker

Could you briefly introduce yourselves and describe your current academic focus?

P: I'm Philip, 26 years old, and I'm currently working on my Masters in Computer Science at the ETH Zurich. I'm especially interested in topics and projects related to artificial intelligence and security.

N: I'm Nikolas I am 26 years old, and I'm studying my masters on Strategy and International management at HSG. I am interested in enabling social responsible companies to reach their full potential

Philip, could you briefly describe in your own terms what a Voice Assistant is?

P: A Voice Assistant is something that reacts to my voice and does some pretty basic tasks. I mean that's right now. I would like it to learn from me. But that's not possible yet.

N: I agree with Philip. A Voice Assistant to me is another form of user input, in any electronic device. It helps me navigate its interface.

Nikolas, to your best knowledge, what is a VA (Voice Assistant) capable of executing?

N: According to my experience, it is able to execute simple tasks such as writing a text message, opening apps—which is generally better if the App is native—making phone calls, that's basically what I've used it for.

In terms of these interactions with technology, where do you see these systems going in the future? What do you want them to be able to do for you in your daily life?

P: I think they should become more and more an extension of our mind. Support us in that sense. Make our life easier without replacing us. And, as I said before, be able to learn and improve themselves.

Do you have any specific functions you are hoping for? Or are you hoping for the device to decide which functions are relevant?

N: I would like it to be more capable of actually doing stuff, instead of being so limited. With the limitation right now—only doing what I described it as doing a moment ago—it's really just a gimmick and doesn't replace my interaction with my mobile. So, for the future, I would like it to be able to actually replace my interaction with my phone—as in touching the screen. It should be truly voice controlled. I'm not so much looking for the voice assistant to predict what I want to do. I think it's **more important** for it to be able to do **what** I want it to do first.

P: I also think understanding us is important. That's a feature I really wish for. It should understand us and not only the patterns of—

N: You mean on a philosophical level? Or what we say when talking to it?

P: No, understanding the context, as in everything you're saying. Maybe. I'm not sure about philosophical. Right now it's just predefined things it can understand, but that's it. If you ask it, for example, show me IT companies in Zurich I can apply to, it's lost, right?

That would actually be an interesting command, because it would have to search for your uploaded resume on LinkedIn, and then match you to jobs that are relevant in that area.

P: True. But, even if I just ask for companies, it needs to—more basically—just figure out which company does what.

Concerning the current status of VAs today, what do you know they have access to when you use them?

P: I have heard that they record basically everything. But, to my knowledge, it is not stored. They just take some information from what they record.

N: Wait. Access in terms of the access they have to us, or the access they have in the system?

I think both are important.

P: I agree. They have access to the browser, and they track everything.

N: I think in terms of personal data, I would like to believe it has access to me talking after I command it to talk. In terms of internal access, it should be something that should be first allowed to have 100% control over the phone—as to what it can access and what it can search. Because now they don't, they have some access. For example, I use android, so the "Google assistant". It has access to a lot of features that are integrated into the system, like Google apps. But the moment that starts interacting with third-party apps, it's not useful anymore.

Philip Junker
Ok Google, where am I now?

Oh, it knows it! Oh, no it's wrong. Contour AG—no, but it's the right address.

Nikolas Molyndris
Ok, let's try something else. Ok Google, where is the Süd bar?

Philip Junker
Haha, mine is also doing it!

The "suit bar" it asks?

Nikolas Molyndris
But how do you . . . mine is in English, do you have it in German?

Philip Junker
No it's also in English.

○
○

Nikolas Molyndris
But nothing matches.

Philip Junker
Ok Google, you are useless.

○
○

Ask her how she feels about Alexa.

Philip Junker
Ok Google, how do you feel about Alexa?

Nikolas Molyndris
He asks so sensitively.

○
○

*I think that's the same answer that Siri gives.
[human error: Siri has a different response]*

Philip Junker
Yeah?

Ok Google, are you the same as Siri?

○
○
○

Nikolas Molyndris
Ok, fair enough.

You both have android-based devices, so you both use the google assistant?

Philip Junker
Ok Google. What's on my screen? — [muted response from VA]
— It's bad, "nothing found."

Nikolas Molyndris
Ok Google, can you take a screenshot?

Nik's Ok Google
Ok, taking a screenshot now. Want to continue?

-
-
-
-
-
-
-

Nik's Ok Google
is unresponsive

-
-
-

Nik's Ok Google
I found a few places.

-
-
-

Philip's Ok Google
I'm sorry you think that. I can do a lot.

-
-
-
-

Philip's Ok Google
Alexa has such a soothing voice, I like it.

-
-
-
-
-

Philip's Ok Google
I think you've reached the wrong virtual assistant. To talk with Siri you might need an iPhone.

So, considering our little experiments, do you have any concerns when you're using your voice assistants?

N: I don't, because it's so astonishingly stupid that I don't think it can do something to hurt me— at any point. You know, actually, it's rare that it hears me and asks me if it should send the text message. I don't know, maybe it's the pronunciation—maybe it's the accent.

P: Yeah, I agree. Right now it's similarly dangerous to have it in your pocket unlocked and having it just press some buttons. It's very random, and it can happen. I currently have the tracking on Google activated, so I track myself wherever I go. They know everything about me.

I've found that there are actually a lot of potential problems with voice assistants concerning infringements of privacy, because of this randomness. Considering privacy, let's turn to our presence on social media. Is a lack of division between privacy and publicity even still of concern today?

N: I think subconsciously, no. But, I think consciously, it still is. If you ask about publicity, people get annoyed when you say, "Oh, this is going to be seen by this and this." I think the further you are away from the perceived problem, the less you care. So, if I say I have a naked picture on my phone, and Chris will see it, then I would care. But if I have a naked picture on my phone and a random "dude" in India will see it, I won't care so much. So in the end, it's the same. I think it's the perceived distance in some cases that makes a difference. Not that that ever happened, but—

P: Nice example—Yeah, I agree. Definitely it's a security concern. But people only start to care when something really happens.

Younger generations in particular are on apps like musica.ly, Snapchat, Instagram. The question is: —if this digital content is accessible in so many ways, and we also agree to the terms of services readily, because it just makes life easier—then: One, is there anything truly private anymore? Two, do we even need to be concerned about privacy?

N: I can let Philip start with this because I always start saying something and then he always says, "I agree."

So let's hear his original ideas first.

P: I think from a technical standpoint what makes it less bad—the privacy thing—is that there is so much data, that a single human being can't possibly go through all of it. Then it's mostly analyzed by machines and generalized. The individual on his or her own doesn't count as much. So I think privacy isn't that much of a concern.

N: What comes to my mind is, that in the past years the data we've produced as humans has stayed the same; considering how we can measure it. But systems now are able to measure them differently. I think privacy is a concern in the sense that if you can measure all this data, in these new ways, you can find more information than even a person knows about him- or herself. Then it might be a concern. I mean, it is a concern, but it might be a problem.—
.....



“...it would be interesting to consider countries where the internet is **censored.**”

Zurich, April 10th, 2018

I met Cristen Anderson last summer, June 2017. She stayed with us while she interned at Google. Cristen is equally as tech savvy and intriguing as Andrea, and during her stay we had many conversations about technology and coding; often while out on hikes. As I began to reflect on my interviews for this magazine, I realized I hadn't yet found a female voice on the topic. That, in fact, I didn't know any female programmers aside from Cristen. I began to contemplate the reason for this disparity. After all, it seems like so much effort has been made in the past few decades to engage and include women in the space of technology. So why couldn't I see these effects personally? Why didn't I have more women in my direct circle that I could immediately call upon? It raised various questions for me personally. Do I simply lack diversity of interest among my close friends, or is there still a significant imbalance? Although this lack of female representation was not the focus of our conversation, I felt that her voice was needed to balance the scale. Cristen offers a fresh perspective on data security, while referencing a global perspective that hadn't yet been considered. As we spoke, we kept the conversation casual, while still revealing some pivotal discussion points within the political aspects of network connectivity and surveillance.

Cristen, can you tell me a little bit about yourself?

C: Yes! First though, thanks for the interview, I'm looking forward to discussing these topics. I am currently a student, and I'm finishing up my degree in Computer Science from UCLA, in June. I'm currently taking a course on computer security, which has taught me lots about current issues in that space. I've also had two internships at Google as a software engineer, one of which was in Zürich, where I've been exposed to how a large company handles security internally and in their products. My main interest right now is software development.

Awesome, so I'll dive into the questions now.

C: Yeah I hope I'm qualified to answer.

Oh, absolutely! Well, the thing is I haven't had any women yet, and this is a really big gap in my research. Although, it's representative of the industry too.

C: Yes

How the internet functions—the protocols that are involved in computer networks etc. —is a very intricate process. What I'd like to know is, how much do you believe the average user understands about these connections and the functions of computer networks?

C: Hmm, very little. I think most people have no idea how it works. They have no idea, even on a basic level, how the internet works. They don't understand what it means when things are in the cloud, or what it means that data is transferred wirelessly, versus through a wire—the fact that the internet uses cables, fiber optic cables—that there is hardware involved in it somewhere. Or the fact that your request is being sent to somewhere across the globe, potentially. You're not even sure exactly where your data is going, or exactly which physical locations it is arriving at, because it's not always a direct journey either. Sometimes, when you're trying to pull up a website it goes to other websites in between too. These are things that you wouldn't see as a user, unless you were looking at it with a specific level of technical precision.

Do you think there are certain things that users should know about? And if so, which ones?

C: Yeah, it's a hard question, because on some level it feels like: “well, I don't need to know how a light switch works to turn on the on my lights.” If you did need to know that, you would say it's probably a design flaw of the light switch. It should be simple to use and you create it in such a way that it is user-friendly. I shouldn't need to know the inner workings of it, in the same way that in order to drive I don't need to know exactly how the engine works. In most other technology it's the same. There are experts in the field that need to know how it functions and operates, and then there are the users. You would hope that you design it in such a way, that your users don't need to have the level of knowledge the expert does to use it. I think this very technical knowledge is something that you won't be able to just explain and understand as someone that is not very technical. So, it feels like there's not really a point in trying to educate people on things that are very complex and perhaps not worth their time. But, I think people do need to know the general privacy and security implications of technology. They should have some awareness of that when they are using it. In the same way that you need to know, when you drive a car, that “Oh, the tire might breakdown”, or that the engine might overheat. You need to be aware of the potential problems. So, knowing some general principles and airing on the side of caution is really great. Though I'm not really sure how much education helps. In the sense that often when there are issues of privacy and security, it seems to only affect a few people in scale. So, if you don't hear of any friends that have encountered identity theft, or been targeted in a phishing attack, then you kind of feel like: “most likely that won't happen to me. So, it doesn't matter what I do on the internet.” It's hard to convince people to care. But, you need to know that when you transmit information over the internet, there is always a risk of it being intercepted. There is always the risk of not being private. But, I also think people know this, but don't really understand the implications of it. They probably think “Ok, so sure in theory someone can do that”, but what would happen if the government had the knowledge on where I've been over the last five years due to my phone's location. What implications would that have for me?

Just knowing that that is a possibility is something that users should be made aware of, so that they can make that choice. So that, if they say: “well I don’t care, I’m just going to leave my location services on because it’s useful to me.” Then at least they are aware that, that data could be collected for some unknown purpose.

So, do you see there being potential ways to educate about security? Or what would you suggest as a possible way of educating people should be in that sense?

C: hmm

It’s a hard question

C: Yeah, well I think that having real-life scenarios is often the easiest way to think about it, because it really underscores its importance. For example, imagine a world where the government had all this data and was tracking everybody and knew where you went to get coffee this morning. Bringing the conversation back to the idea that “this is a possibility in the world we live in”—that it’s not just science fiction.

On that note, when you think about series such as, “Black Mirror”, does technology’s role in entertainment obscure the fact that even though much of it is sensationalized, the basic concepts upon which the episodes are built, are in many ways possible realities—or already are realities. In other words, does pop-culture desensitize the issue?

C: Yeah, I think people just don’t tend to think about it that much. You’re just like: “Oh, everybody is doing it, so it must be fine. This is just the world we live in.” I feel like it is also hard in terms of education, because it’s hard to offer any solution or any steps you should take. In a lot of ways, we’re just so dependent on technology. I can’t just tell you to never use your location services on your phone, because you need that for a lot of things and that would be highly impractical. So, I guess for education, I would especially focus on how insecure the internet is in general. I would also focus on the awareness of the way that tech companies and governments use data, and how it is a big business.

[...]

The last couple of weeks Facebook has been facing scrutiny due to its lack of protection of privacy for its users. But, what I’d like to know is: considering our presence on social media, where there seems to be a lack of division between privacy publicity—is privacy something that we should even still be concerned about?

C: Yeah, I think it’s a good question for everyone to think about for themselves. Just to consider, you know, in life almost as a philosophical question. What is it about me that I consider private and public? I mean so many of our relationships end up on the internet with messaging. To some extent, there is a lot that isn’t private, and some people’s perspective is: “well, I don’t have anything to hide, you know.” or “I’m not doing anything illegal, so why should I care.” But, I think you’re

right that in general there are a lot of areas where there is now just no privacy in that space. I think people are also just not as aware either. They still consider—the internet, social media—to be a private space, even when it’s not. So, there is a disconnect that in terms of how people perceive their privacy, and how their reality actually is. I also think it would be interesting to consider countries where the internet is censored, and how people get around and end up having a lot of privacy in their private life. Because, if they didn’t—well in western countries whatever it is may be legal—but in their countries, it isn’t. They are concerned about that, so they tend to be more aware of what is private. I feel like the lack of division is more of a problem in developed countries, where generally you are somewhat trusting of your government—and other western companies or entities. So, you’re less likely to be concerned about how they are viewing you, or what they are doing with your data.

That’s a really good point. That’s a really, really good point. It would be interesting to hear a perspective on that.

C: Yeah, for example when I talk to friends from China, it’s a whole different world with censorship. People just do tend to be more private, and more aware of “if this is on my social media, the government could use this against me and there could be real repercussions.” People are more concerned with it in that instance.

You also mentioned the perception of private spaces. How do you think user design, user experience, has contributed to that? Do you see there being a possibility on that end, to improve our sense and awareness of privacy online?

C: Yeah, I mean I think all the social media companies would like you to think that your messages are private and that your images are stored securely. They definitely key that in to their language and user experience, in the way that you use it. In the sense that it’s clear you’re sending a message to only one person, and you’re not sending it to fifty people. I guess theoretically, yes there are ways to make that more obvious, but that would definitely not be in any companies business interest to advertise. I mean what would you say, “oh, you’re sending this message to so-and-so, and our servers.”? Or, “when you’re liking this post, the ad-company is able to view this and is tracking you.”? It’s hard, because it’s just not in the company’s interest to tell you that. Nobody wants to think about it unless they have to. Or “your message is now stored on this machine in Nevada, and this technician is servicing it.”? You know, there are things that are more secure than others. There are ways to be a lot more private on the internet. I’m sure you’ve heard about secure connections versus insecure connections. So, whether it’s encrypted, that’s something that could do to improve your security. But, while there are things you can do, there will also be things you are less aware of.

That also circles back to your point that it should be user-friendly too. There are some things that the average user really shouldn't have to know about when using a device or service.

C: mhm, exactly.

You mentioned something before about how many of our relationships are online, through social media or even just e-mail correspondence. Could you expand on that position a bit? What strikes you about that shift?

C: Yeah, originally how things are with relationships, is that you have a face-to-face relationship.

What goes on between you and another person is only known by you, and it's private in that sense.

But, since this relationship is now carried out online all these other entities have insider information about these relationships, which tend to be pretty personal things. I think in a way it's an unknown, in the sense that: "what does it mean that Facebook knows the top 5 people I interact with?" I think it really hasn't been abused to an extreme extent at this point.

But, I could see it being dangerous with a more totalitarian—for example, if Facebook has all this data and were to be hacked by China. Then China can say, "here are people that are anti-communist and then here are their top five friends", you know? It's very easy to then find that network of people, far faster than just trying to figure it out through word of mouth.

So, I think some of these questions seem to be less relevant to us. Or at least we **think** they are less relevant, being in a developed country and in a place where we don't think the government is currently misusing our information. But, just thinking about how this information is out there, and that all technologies have had vulnerabilities and continue to have vulnerabilities to attackers—what this would mean is that somebody who was out to get me, they could find out who I interacted with the most based on this messaging trail. Which they wouldn't know if your relationship was conducted outside of social media. That's the thing that kind of stands out to me.

Like you said its still an unknown in a sense,, because in other countries you might be able to imagine how it could be used against you. But, this is information that they do have on us and until it becomes exploited in some way, we won't really know how they might do this. There are so many possibilities of what that could look like.—As a final question, do you think anything is or can be truly private anymore?

C: Well, I feel like there **are** ways to stay off the grid still. So, in that sense yes there are ways to be completely detached from technology. For example: do not own a phone, do not have a computer. There are many people in the world who still live this way, and in comparison, their lives are probably relatively private. There are still lots of people in the world that don't have internet access. So, I would say their lives are relatively private. But, I guess the question is referring

to whether it is possible, in the developed world, and our current context to have things that are still private. I think to some extent "no", I mean even if I'm meeting up with my friend I bring my phone, and that has a location tracker. They are probably bringing their phone too, which also has a location tracker.

So, somebody is able to know that we met up.

If you abstain from technology though, that would then be relatively private. But, even then you need to think about where you are. Are you somewhere with a bunch of surveillance cameras, or are you really out in the wild or something? Because it's not always just you, it might also be the society you live in that's tracking you.—

INSPIRATION.



“...in security it is totally wrong to say there is no risk.

What you want is to minimize the risk...”

Rüschliko March 11th, 2018

This second part of the interview with Andrea Mambretti focuses on issues of privacy, hack-ing and the role of voice assistants. Following the first part of the interview, which focused on how the internet works, we begin to discuss the role this has on our use of mobile devices. Andrea begins to explain how certain aspects of our seemingly secure and harmless connectivity to the internet can become vulnerable and an object of concern.

So could you briefly in your own words define what a voice assistant like Siri is? Then maybe also describe what it does?

A: So mechanisms like Siri are speech recognition systems. They are based on speech recognition Software and what they do is listen through a microphone. So, they receive the input from the microphone, and they sense when they can parse something that is known to them. The first application of these systems were mechanisms for accessibility. Things like emulated keyboards that worked based on speech rather than keystroke, for people that couldn't type. Then this evolved into something more interactive, like Siri. Siri is partially built on speech recognition, but it also has this very complex machine learning component that is based on the inputs it receives from the microphone. It reacts and gives you information or reacts and does some action, like opening some manual or opening an application. This is all based on some kind of machine learning—I mean generally, I would assume some sort of neural network. I'm not sure. I personally don't know, because it's a company secret.—What the company does with these elements is train them to have a wide knowledge of assistance, and they provide you a service that is like an automatic helpdesk for anything you want.

To your best knowledge what is a VA capable of executing? You mentioned that the program is built on machine learning fundamentals, so I would assume this means that its capabilities expand the longer it is running.

A: The capabilities of such a system are based on how much it has been trained. Every machine learning based algorithm requires a phase of learning, based on sample data. Based on how much data is in this training set, the more your neural network will know various choices and actions. Then what they

do is whenever you use them, they have a certain feedback loop that adjusts the answers, based on what people expect. So what the company does is that they have a beta period when people use the devices, and these people then give feedback based on the actual results. For instance, you ask Siri to show you the way to the next grocery store and instead she gives you the directions to the movie theater. You might say, no this is not what I want, and then you would type the answer you were expecting. The system will adjust itself for the next time you ask it the same question. This procedure is done on a large scale, on an Amazon scale, Apple scale, Microsoft scale. You have tons of users that use the devices all the time, so they provide the best data set you could possibly have. They also have programs to incentivize participation by raffling off devices for free; all you do is subscribe and test for the company. It is just another pool of people for the company, but these people can benefit from these testing phases.

So in terms of our interactions as they stand today, where do you see these devices and systems going in the future? And what do you hope to see from this development?

A: These systems definitely are the future. Because they provide a new way to interact with our devices. People adjust to them, because it is much easier than using their keyboard. There are many cases where it's just easier to talk to the phone, than to interact with your device by tapping on it. As users we generally tend to go for the easiest path. This is why these systems keep getting better, because people keep using them. Since this is the tendency, I would expect these devices to be integrated in everything at some point. For example, cars now have the same systems—or they have mechanisms where you can plug your phone in so that your phone becomes the software that is running in the car—and you can ask Siri to take you someplace and give you the directions to that location. Then the car's GPS will show you the map. So, this is already one type of integration. These kinds of integrations will continue. Eventually, it will not even be necessary to plug your phone into the car, it will already be in the car, or in the kitchen for instance, or in our houses in general. You might just say I want the lights on and there would be a speech recognition system, maybe one much simpler than Siri, and it will just turn on the lights. I see this as the future of these devices. They will have a much wider integration in our life and interact with every device we use.

Considering this vision of the future, if they are integrated and they do have access to so many things, where are the dangers or the pitfalls? Do you see there being ways to secure against possible breaches, or is it too early to tell?

A: Well just like everything that is widely used, they, of course, attract the interest of malicious people—and malicious attackers as we would call them—because data is very important these days.

The data that we are now sharing on the internet is becoming more and more sensitive, because everything is moving to the internet. So whatever was in your wallet before, is now on the internet. The more these devices and systems get integrated—which already have a lot of your information—the more the security of these new components is going to affect the overall system.

“...the security is going to be paramount for these types of devices...”

Therefore, as for everything else, the security is going to be paramount for these types of devices. What I am trying to get at is, that even though you have a system—made of different components—and you can be sure that each of these components by themselves is secure, does not guarantee that when you put them all together they will be secure. In fact, the more you plug, the more you connect and the more ways to bypass the security of the single one. Since they were designed in an isolated setting, they were not meant to work together. This then creates problems, because you have new ways to attack.

Generally, something is attackable, if an attacker can actually interact with components. So, if a component was designed to have zero interaction with the external world and then you plug it to the internet and allow people to actually interact with it, you cannot guarantee security—unless you redesign or make sure this change this component so that it will not affect the security. This is what happened to computers in the first place. The network/internet was invented fifty years after the first computers. Computers and programs were fine until they became connected to the internet, initially they were not meant to connect. This software is now running on a remote machine and can be interacted with. Now you can find a way to access this machine, since this software was not designed with the internet or any type of connectivity in mind. This was, for example, the concept behind the Morris worm back in the 70's. A guy from MIT, who is now a professor there, wrote a software that used a vulnerability that he discovered in a software package that every computer in the network used. So he wrote this software that connected to each of these computers. It would test to see if that package was installed and if it was, then it would infect the software and the new machine would start the next attack. It was called the Morris worm, because it spread around like a worm and would clone itself in the next machine. It took down their internet/network, this first version of the internet. When he wrote the virus, he didn't write a control into it, to test whether a machine had already been hacked. So what happened is that every time this worm was attacking a machine, it was attacking no matter if there was already a copy of it on the machine or not. So each machine continued forwarding the hack over and over again, until the

network could not support the traffic anymore. They had to shut down everything. He was the first guy that risked jail to provoke DoS (Denial of Service).

Denial of Service is an attack in which the goal is to make a service unavailable to its users. For instance, a website that is not answering to connections and therefore results not reachable anymore to a user. These kind of attacks generally aims to exhaust some of the resources of the service to make it not functional. Usually they require the large scale control of a lot of machines that will all together communicate with the service reaches his maximum level of operation causing it to fail and therefore becoming unavailable. The most common resource used to DoS is network bandwidth

I mean the systems we are talking about these days are so complicated and distributed all over the globe, that making sure they are secure is a huge amount of work. Plus, it's very expensive work. Sometimes, it takes more time than is required and you may still be attacked, or have vulnerabilities. We use so many components in software these days, and they are considered secure. But then maybe there is a zero day—which is a term for a vulnerability that no one has discovered yet—and then there is some guy that discovers it and is on the other side as the attacker. He might want to use it as long as no one knows about it, to achieve what he wants. Then comes the point where he is detected, and so we patch everybody. But, there is this gap between when this vulnerability is discovered and is used, and when it gets patched.

There was this vulnerability, "Heartbleed", back in 2014. It was in the open SSL library, which is the crypto library that everybody uses. There is almost no piece of software that doesn't use it. Google, Facebook, they might have their own implementation, but the base comes from this library. Basically, 90% of the internet was hackable in a very serious way. Most of the big companies like Google, 12 hours after the discovery of "Heartbleed", had already patched every software that they had. They had the man power, and they organized almost an infinite amount of resources. But, a normal guy that is still using the old version of open SSL is still running that same issue. If he doesn't know how to update his system, or his system is too old to be updated, then he is going to run that vulnerability forever. So sometimes it's not even possible to achieve full security. In companies there is a huge problem, because every company has their own way to assess security issues. However, then they might buy software or integrate their software with another company's which has different standards. In that case security becomes a constant problem, because you might not get the code for the software in order to easily verify its security. It is very hard to then identify if there is a vulnerability. So, the question is how much do you want to invest to verify that someone else's component is as secure as your own. In the end it's a tradeoff that many companies have to deal with every day. Maybe you don't have the manpower to buy that part, but you just have to buy it.

Then you're compromising your standards of security. There are so many levels of things that you need to check and that you have to make sure are secure. And then, even if you can prove that all the pieces of software you run are secure—that there is no way for an attacker to interact with the system from the outside and actually hack it or get information from it—then you still have the last piece that is always vulnerable in every company, which is the person—the employee.

In many cases it is much easier to circumvent the employee, rather than finding a software vulnerability. There are ways to train your employees, but then maybe you have an employee that wants to leave the company—like Snowden.

So, what you're saying is that nothing is ever 100% secure.

A: No, in fact in security it is totally wrong to say there is no risk. What you want is to minimize the risk. So, each company and everyone that works on software, we all try to use the best practices, such as: invest in security components, security training, security evaluation, penetration testing. These are all investments that lower your risk, but you cannot nullify the risk. You just need to deal with it. What you want to do is invest enough money, so that in case of a breach what you are going to pay due to the breach is lower than the fine you would pay. You want to make sure that what you are protecting is worth the money you are spending.

There are two things here. There is, data collection and data security. But on a more social level, considering our presence on social media and the things we are willing to share with each other, there is a certain lack of division between privacy and what is made public. Is the divide between these two spheres still of concern today? It seems that with sensitive data, such as identification information, we still desire this to remain private. But, in terms of everything else—

A: Yeah, so social networks—this new way people started to interact with each other—changed the perception of what we are willing to share. Everybody has their own level of willingness to share personal information, personal experiences and everything that is related to what we generally know as privacy. Before the internet, or before every social network, people had a very practical sense of what they wanted to share and what they didn't want to share. [. . .] For instance, we are discussing in this room, I am sharing something with you, and I know this is going to be between me and you; that's it, and I decide "do I want to share this, or do I not". It's a decision that I can make and it's very easy to understand the effects of my decision. On the internet on the other hand, there is a sort of detachment between what you write, or what you share, and who is going to receive it. A lot of people have a very hard time realizing that what they actually share there, is much more than what they would be willing to share in a situation in the real world. If they

would have had the same amount of people in front of them, they would not share the same things. But, the internet and social media have removed this, detached the person from the real situation. Social media and the interaction it allows today is making a lot of information that is not supposed to be public, public. Even small amounts of information, though they might not seem really important—people forget that the internet does not forget. If you share this piece of information today, and then share another small piece tomorrow, and in 20 years you share a little bit more, someone that is able to listen to this, and will be able to put them all together.

So, even though this information by itself is not revealing, you put it all together it becomes much more meaningful than we thought before, and might actually affect our real life. A small example is people that use social media to describe what they do every day. The might just say "oh, today I woke up", or "this is my cup of coffee", or "oh, I'm taking the train at 8:50, as always." These are small bits of information and its someone's normal life. But, if they are publicly shared and I'm listening to this information, then I check one day, I check two days, I check maybe for a month and I know exactly when you are home and when you are not. I even can know when you're on vacation, or what you are planning to do. So, if I want to rob your home, now I know exactly when to come, and how much time I'm going to have. Maybe you're even revealing information about the house itself, because you are sharing pictures of your place. So maybe from one picture to another picture I know, "oh, there is a cabinet, maybe there is a safe." And this is now all available online. You just have to be patient enough and listen. Many people have been robbed in this way. Based on the information you give to people, everything is possible.

“Very few people spend enough time in the settings to understand what exactly is going to be public and what is not.”

Do people then have a false sense privacy and security, based on social media?

A: Yes. In many cases, because sometimes there are misconfigurations on, or changes to the website itself. The company might try their best to let people know that they've changed their settings, but the normal user might not have time to read through all the changes, so they just accept the new terms. Very few people spend enough time in the settings to understand what exactly is going to be public and what is not.

But, the thing is even though the tools are there to control privacy, how many people spend even just 10 minutes to look at the options they have? I can bet less it is than 30% of people. Plus, then you have to consider the integration between social networks. So maybe you are secure on facebook, but then you have this aggregator that posts on twitter, because you want 'Retweets' and not only 'Likes'—and twitter is public. Or maybe you have Instagram, and then by default most of the pictures are public. [. . .]

Another thing I found scary last year, was this function on Facebook. My girlfriend—I was back in Italy—and she was touring around with her friends in the grand canyon area. Whenever she was texting me I noticed the messenger app, by default, was revealing the exact last location she was connected to.

Really?

A: Yeah, for the whole trip I could say: “oh, you are here right now”—with the precision of like, Paige, Arizona. It was all in the message info.

(We check to see if this is still possible)

A: Yeah, I don't know about the iPhone. On Android it would come up when you were offline. It would say, last connection from “Paige, Arizona”. I could pin every point that they were camping out at. I was skeptical.

I mean in terms of hiking this location feature is probably a good thing.

A: Yeah exactly. But, she didn't know that all her friends could see where she was. So, I told her: “well, you might want to deactivate this.” It was just an option Facebook had built in, but why activate this by default. Lots of people don't even know about this stuff, or they don't pay attention.

So, do you think anything is truly private anymore?
Do we need privacy?

A: Even if we think that we don't, it's not good enough to just give it up, even if you think: “I don't have anything to hide, that's not a good enough reason to just give it away.”—



**“SICHERHEIT
WOLLEN ALLE,
SIE IST ETWAS SCHWER ZU SPEZIFIZIEREN
UND DU MERKST ES VOR ALLEM ERST
DANN WENN DU SIE NICHT HAST.”**

Zurich, March 7th, 2018

As it so happens, just like our online profiles, we develop networks through social connections and referrals. One evening, while I was explaining my thesis to a friend, she suggested I reach out someone she knew. After contacting Umberto to set up a meeting, I launched a quick google search, only to realize that this ‘friend working in data security’ was actually the president of the Information Security Society of Switzerland. We are now sitting at the “Time. . . Café and Lounge” in the Zurich main train station. The turbulent atmosphere around us leaves us enveloped by a cacophony of voices. To a certain degree this environment is challenging for our conversation, and creates nearly impossible conditions for a recorded interview. However, it feels like we are in a David Fincher scene, where the background noise has been intentionally added with the goal to give weight and importance to the conversation. At the same time, it feels like the loud commotion veils our conversation, creating a barrier between us and others. Umbi begins to answer my first question speaking loudly over the crowded atmosphere.

Erzähl mir noch ein wenig über dich. Du arbeitest in Sicherheit und Datenschutz. Aber in welchem Unternehmen arbeitest du und was ist deine Rolle dort?

U: Gearbeitet habe ich bis jetzt die letzten drei Jahre als Berater im Sicherheitsumfeld für bestehende Finanzunternehmen. Jetzt arbeite ich seit Anfang Monat bei der Six Financial Information. In der Abteilung: Börse, Zahlungsverkehr, aber im IT und Informations Sicherheit Bereich. Das beinhaltet auch Datenschutz und rechtliche Anliegen. Aber in diesem Bereich bin ich jetzt schon 15 Jahre tätig. Von meiner Grundausbildung her war ich Wirtschaftsinformatiker. Zuerst machte ich eine Lehre und dann eine Weiterbildung. Ich mache das Ganze daher jetzt auch seit 25 Jahre. Seit 15 Jahren bin ich ausschliesslich in der Security Branche tätig. Ich mache das geschäftlich aber auch als Hobby, im Sinne von meiner Dozententätigkeit und innerhalb von Vereinen, die das Pflegen - national sowie international. Also ein wenig Hobby und Beruf, beides miteinander.

Also in diesem Fall bedeutet für Dich auch das Akronym GDPR etwas?

U: Ja, ja

Was bedeutet das GDPR (General Data Protection Rights) denn ganz genau für die Systeme, die es in der Schweiz dafür/ dagegen schon gibt?

U: GDPR. Das ist die neue, bzw. total überarbeitete Gesetzgebung für Datenschutz. Vorher war das eine Richtlinie, 95/46 ist die jetzt geltende Version. Es ist ja eben kein Gesetz, sondern eine Richtlinie. Das heisst die Länder, also die europäischen Länder müssen irgendwas umsetzen in diesem Bereich. Sie können sich anhand dieser Richtlinie orientieren, müssen es aber nicht zwingend so machen. Jetzt, das GDPR also auf deutsch: Datenschutz Grundverordnung, ist nur eine Vorgabe. Sie müssen es mindestens so machen, dürfen es noch schärfer gestalten, wenn sie Lust haben. Aber diese Bestimmung wird einfach ab dem 25. Mai 2018 gültig. Die Eigenheit dabei ist das ein paar neue Sachen dabei sind - ein paar schärfere Regelungen. Eine der krasseren Regelungen sind die massiv hohen Bussen bei nicht Einhaltung und dass diese auch ausserhalb Europas gültig sind. Also, das heisst sobald du Daten von EU-Bürgern bearbeitest, unterstehst du diesem Gesetz. Das heisst es wird besonders viele Schweizer Firmen betreffen, die auch EU Bürger Kunden haben.

Aber wenn man diesen Datenschutz brechen wollte—

U: Also du meinst, wenn jemand es bewusst nicht einhalten möchte?

Genau, also wenn man die Server ausserhalb der EU betreiben würde?

U: Also, das geht dann eben nicht. Es kommt nicht darauf an wo die Daten effektiv sind. Das ist dann auch der Punkt. Das Reglement ist geltend, sobald du Daten von EU-Bürgern bearbeitest. Wo du das dann machst, spielt keine Rolle. Es ist ex-territorial gültig, das ist auch das Spezielle daran. Meistens sind Gesetze innerhalb von dem entsprechenden Land anwendbar und geltend. Aber natürlich sind hierbei auch wieder gewisse Bedingungen erforderlich. Eine Schweizer Firma muss dann in Europa eine Repräsentanz haben. Aber wenn du einen Verstoss dagegen machen möchtest, kannst du nicht damit rechnen dass du es einfacher hast wenn das nicht der Fall ist. Denn die Europäer werden dann Druck aufsetzen um zu versichern, dass du dich daran hältst. Man ist sehr gespannt wie das dann wirklich auch umgesetzt wird, denn es ist erst im Mai gültig. Erst dann wird man sehen können, wie fest sie es dann auch durchsetzen.

Kannst du mir noch mehr über die Massnahmen und Bussen erzählen?

U: Die hohen Bussen sind recht absolut. Die Firmen fragen sich deshalb jetzt schon was sie unternehmen müssen und wie sie die Daten abzusichern haben. Das war weniger wichtig vorher. Den Datenschutz hat es zwar auch schon gegeben, aber der wurde nicht besonders ernst genommen. Wenn man dagegen verstösst, musste man als Firma nicht bluten.

Nehmen wir zum Beispiel die Swisscom. Sie hatte vierzigtausend Kundendaten verloren bzw. wurden ihnen geklaut. Sie haben erst drei Monate später diese Informationen veröffentlicht und haben getan, als ob es nichts wäre. Das kann man sich dann mit den neuen Regelungen nicht erlauben. Man kann das immer noch in den Medien schön reden lassen, aber zu zahlst dann einfach 2% von deinem Jahresumsatz an Bussen. Das ist dann eine Summe, bei der ein paar Millionen für vorbeugende Schutzmassnahmen, auch wieder Sinn zu machen scheint. Bis heute noch zahlt mal eine Busse von 10'000.- CHF wenn es soweit kommt. Für eine Grosse Firma ist das ja nur ein Tropfen. Du wirst dir deswegen keine zusätzliche Mühe geben. Das wäre genau so als würde man sagen: «man soll nicht zu schnell fahren, aber wenn du zu schnell fährst, kostet deine Busse nur 10.-.» Dann fährt jeder gerne 250km/h. Hier in der Schweiz haben wir massive Bussen, deswegen halten sich auch an die Verkehrsregeln. Die Schweizer werden also ihre Massnahmen anpassen, aber nicht mehr dieses Jahr.

Wir beziehen uns jetzt aber eher auf Schweizer Firmen, wie sieht es denn für Unternehmen ausserhalb Europa aus?

U: Europa ist sozusagen die Wiege des Datenschutzes, im Sinne des Persönlichkeitsgrundrechts. In der restliche Welt hat man das so nicht. Zum Beispiel Amerika, das ist eines der Länder das das Prinzip vom Datenschutz so gar nicht kennt. Was natürlich eine Reibungsfläche ist. Die meisten grossen Anbieter von Informationsdienstleistungen mit entsprechenden Cloudservices wie, Google, Amazon, Microsoft, sind nun mal amerikanische Firmen. Was du in Amerika problemlos kannst, ist in Europa nicht möglich.

Aber auch die amerikanische Firmen werden sich an den GDPR halten müssen. Wenn ich einen Apple Home bei mir Zuhause einrichte, dann landen die Daten letztlich auf dem amerikanischen Server, aber 'Ich' bin ein Schweizer Kunde. Deswegen haben sie sich auch, wann immer möglich sich an Schweizer Gesetze zu halten.

Aber das heisst eigentlich, dass sie Ihren Server irgendwie spalten müssen?

U: Entweder so, was sinnvoller ist. Sie unterscheiden dann die Daten, denn die amerikanischen Daten können sie liegen lassen. Aber bei den Europäischen, da müssen sie vorsichtiger sein, denn das könnte sie dann richtig viel kosten. Oder sie sagen: Nein, wir schützen alle Daten gleich gut wie die Europäischen «Weil, wenn schon, denn schon». Sie hätten noch weniger Probleme wenn sie gewisse Systeme in Amerika gar nicht aufstellen.

Entscheidet sich Amerika auch neue Datenschutz Massnahmen einzusetzen oder ist das Ihnen nicht wichtig?

U: Im Juni wird jetzt eine Entscheidung des Supreme Courts erwartet, zwischen Microsoft und dem Justizministerium. Es geht darum, dass Behörden auf Daten von amerikanischen Firmen zugreifen könnten, auch wenn ihr Server nicht in Amerika ist. Das wäre ein Vernichtungsurteil, wenn dafür entschieden wird. Dann würde man auch gar nicht mehr erst zum amerikanischen Anbieter gehen. Du müsstest nämlich dann davon ausgehen, dass irgend etwas mit diesen

Daten passiert, wenn die Behörden darauf zugreifen könnten. Dieses Grundsatzurteil wird deshalb auch mit Spannung erwartet.

In der Schweiz muss ich eine Genehmigung von einer Person einholen bei Bildmaterial, Tonaufnahmen, und Videoaufnahmen. Man muss immer transparent sein. Also ist meine Frage ob in unserer technologischen Welt die Idee von Privatsphäre überhaupt noch wichtig/relevant ist?

U: Ja, das Problem ist das man ein Persönlichkeitsrecht hat auf Privatsphäre grundsätzlich. Du kannst das als physische biologische Einheit wahrnehmen. Du hast es und kannst dich entscheiden ob du dein Gesicht verhüllen möchtest oder ob du eine Sonnenbrille aufsetzt. Aber deine Daten, die dich repräsentieren, können diese Entscheidung nicht treffen. Sie sind ja keine lebenden Instanzen. Deswegen gibt es ja auch dieses Datenschutzrecht, dein Persönlichkeitsrecht in seiner digitalen Form. Das Problem ist, dass Daten als semi-physisches materielles Gut per Definition hoch flüchtig und beliebig manipulierbar sind. Das heisst wenn du mir jetzt deine Nummer gibst, habe ich sie und sie wird im Telefon gespeichert. Apple wird sie bekommen und man kann sie herum schicken. Idealerweise könnte man deine Daten so kapseln, dass sie auch deine virtuelle Persönlichkeit sind. Statt dass sie einfach flüchtige Daten sind. Sie sind schliesslich nur Zahlen und Buchstaben. Wenn diese Zahlen und Buchstaben eigentlich eine Person repräsentieren, dann wäre es doch schön wenn sie Eigenschaften hätten und so gekapselt werden könnten, dass wir sie selber in der Hand haben könnten. Das ist einfach nicht gegeben. Darum können Daten, und werden sie auch, übermässig missbraucht. Die Durchsetzung dieses Rechts ist schwieriger, denn mit denen kannst du alles machen. Die Daten lassen sich beliebig manipulieren - sie haben keine intelligenten Eigenschaften. Für eine kommerzielle Firma ist der Einbau solcher Eigenschaften auch nicht von Interesse. Denn solange sie diese Daten auswerten können, desto mehr Einsicht haben sie auch in den Markt. Man muss aber auch berücksichtigen, dass die Unternehmen dieses neue Reglement wahrscheinlich viel ernster nehmen werden, als die Regierung das machen wird.

»Das Problem ist, dass Daten als semi-physisches materielles Gut per Definition hoch flüchtig und beliebig manipulierbar sind.«

Microsoft zum Beispiel im geschäftlichen Umfeld ist extrem aktiv im Moment, hingegen hat Google offenbar ein weniger ausgeprägtes Interesse daran. Daher, wenn ich eine Dienstleistung als Geschäft nützen möchte dann kriege ich von Microsoft viel kompatiblere Angebote was europäische Anforderungen gesetzlicher Art bzw. Datenschutz betrifft, als von Google oder Apple.

Du sprichst von verschiedenen Firmen, wie unterscheiden sie sich in ihren Leistungen angesichts ihrer Datenschutzrechts Philosophie?

U: Apple hat von Grund auf eine andere Philosophie als Google, wie auch als Microsoft. Das heisst, ein Google verdient primär Geld mit dieser Auswertung von Daten. Ein Microsoft muss das nicht, sie haben nämlich andere Einkommenskanäle und Apple auch. Das heisst ihr Geschäftsmodell ist nicht «Wir werden deine Daten ausnutzen und verkaufen sie weiter und produzieren Werbung», das ist Googles Modell und Facebook noch mehr. Aber Google ist viel transparenter bei dem was sie machen als Facebook. Facebook findet: «wir verbessern die Welt, aber verdienen uns dumm und dämlich während wir deine Daten ausnutzen.» Google sagt dir: «wir werden deine Daten ausnutzen bis unsere «ohre gwagglet», aber du kannst auch einen Teil davon ausschalten. Wiederum sagt Apple: «wir haben zwar deine Daten, aber sie interessieren uns gar nicht gross, weil wir uns dumm und dämlich mit unserer Hardware verdienen», und Microsoft eigentlich auch. Microsoft hat bisher Software verkauft, und jetzt verkaufen sie Software in Dienstleistungs Form, als Cloud Service.

Eine Cortana hat also ein anderes Interesse als einen HomePod. Google bietet gratis G-mail an, weil sie den Inhalt von allen Mails dann überprüfen können damit sie dir relevante Werbung präsentieren. Das ist der Deal. Bei Microsoft bekommst du dein E-Mail gratis über weil sie einfach finden, «easy-peasy, machen wir doch einfach etwas Gutes für unsere Kunden» und dabei schleifen sie ihr Image schön. Aber bei Apple bezahlst du was, wenig, aber sie sagen «wir haben kein Interesse daran, und es kostet uns viel Geld euch diese Dienstleistung anzubieten». Facebook ist auch gratis, verkaufen dir eine Idylle einer besseren Welt und lassen dich glauben, du willst es so. Aber dabei verdienen sie sich dumm und dämlich mit Werbung. Viele 'verteufeln' Google, und ich sage «klar, nicht alles was Gold ist, glänzt», aber Google, wenn du weisst wenigstens wie und wo, dann ist Google wenigstens noch transparent. Dagegen hat Facebook immer noch einen vorbehaltenen Image der Weltverbesser und du weisst nicht wirklich, ob du daran glauben kannst.

Und wie spielen diese verschiedenen Philosophien dann auf den Home Listening Devices wie Alexa oder den HomePod von Apple aus?

U: Du hast also einen Apple, einen Google, einen Amazon.

Eben, Amazon ist auch ein Laden. Sie haben deshalb ein Interesse an deinen Daten. Ich meine Amazon war einer der ersten, der dieses 'Profiling' gebracht hat in dem sie, anhand deiner Einkäufe, dir Empfehlungen und Angebote gemacht haben. Deshalb interessiert es sie auch sehr, was du Zuhause alles machst. Damit können sie dir noch genauer sagen was du möchtest. Z.B. du sagst 'Kino', und Alexa meint dann «übrigens, in dem Kino am Ende der Strasse gibt es heute eine Sondervorstellung, vielleicht bist du interessiert.»

Apple hat das Interesse in dem Sinn nicht so vordergründig. Das heisst der Apple HomePod wird eher dein Diener sein, ohne einen unterschwelligen Gedanken dahinter zu haben. Die anderen Anbieter haben aber meist noch ein zweites Interesse.

Also, einerseits gibt es den Konsum. Firmen wollen diese Einsicht, damit sie dir mehr anbieten können.

Aber wenn die ganzen Geräte an deinem Haus angeschlossen sind, dann taucht auch noch die Frage von Privatsphäre und Sicherheit auf. Wie kann dieser Aspekt zum Problem werden?

U: Genau, also du hast zwei Sphären. Du hast den Datenschutz, was passiert mit diesen Daten, diesen Verknüpfungen und diesen Auswertungen. Das heisst, wenn ich bestimmte Produkte bevorzuge und kaufe und mit dir dann zuhause ein Gespräch führe, dann geht es sie nichts an, was wir miteinander besprochen haben. Das ist also das Eine.

»Es gibt also den Grundsatz, «nur weil du es an das Internet anschliessen kannst, heisst es nicht dass du es musst.»«

Und dann ist das Andere die Sicherheit des Systems an sich. Das heisst, du vertraust dem System weil, wie gesagt es einen elektronischen Diener darstellt. Ich sage dann «Siri schalte das Licht aus, mach Musik an, und schliesse bitte unten die Türe.» weil ich keine Lust habe die Treppe wieder hinunter zu laufen. Jetzt wäre das natürlich schön wenn sie das auch nur dann macht wenn ich ihr das sage, aber nicht noch auf jemand anderes hört wenn dieser schreien sollte «Siri mach die Türe bitte wieder auf!» Die Frage ist dann: wie kommt man in den System hinein. Wenn sie zum Internet Anschluss hat, dann so. Es gibt also den Grundsatz, «nur weil du es an das Internet anschliessen kannst, heisst es nicht dass du es musst.» Amazon hat ja schon das elektronische Türschloss, dass du über die Webcam fernsteuern kannst um den Kurier in dein Haus hineinzulassen. Elektronische Schlösser, die man durch einen App steuern kann, mit denen man auch anderen ganz leicht die Berechtigung geben kann die eigene Haustür aufzuschliessen. Hoffentlich kannst auch wirklich nur du das.

Das sind die zwei thematisch unterschiedlichen Sphären. Das Eine profitiert aber vom anderen. Zum Beispiel, wenn jetzt Amazon sagt, «damit wir dir immer diese Dienste bringen können, müssen wir uns ständig mit dem Gerät verbinden können.» Das heisst, du darfst es nie ausschalten und du muss es immer am Internet verbunden lassen, auch wenn du schläfst, «aus Gründen». Das Gerät besitzt jetzt aber einen Sicherheitsmerkmal, damit es auch weiss, dass es sich nur mit Amazon zu verbinden hat und nicht noch mit Anderen, die nur so aussehen. Das heisst wenn es das Sicherheitsmerkmal hat ist es keine Sache das so auszubauen, dass es eben auch den Datenschutz unterstützt. Amazon hat vermutlich keine Interesse daran und baut auch deshalb diese Merkmale nicht in das Gerät hinein. Man könnte aber auch sagen «ja, Ihr wollt das Sicherheitsmerkmal nicht, aber ich möchte es. Baut es doch mal so ein das ich alle anderen ausschliessen kann, nur euch nicht.» Aber eben, das so zu bauen, das ist dann vielleicht aufwendiger als nur Null und Eins. Dann kriegen wir die folgende Situation: Ja, wir bauen es ein, aber es kostet 10.50. Aber das will man nicht bezahlen, doch das Gerät finde ich so toll, dass ich es trotzdem kaufen möchte und der Preis den ich dann deswegen zahle ist, dass ich eine gewisse Privatsphäre aufbebe.

Also, ganz konkret, gibt es denn Privatsphäre noch?

U: Die die dann sagen «Ja, der Zug für Privatsphäre ist schon lange abgefahren.» Der Zug ist abgefahren im Sinne von «Hey, ich mache da nicht mit, dann riskiere ich auch nichts.» Also, ich mache keinen Facebook Account, weil dann kann mir auch nichts passieren. Dieser Zug ist abgefahren, das haben wir auch nicht in den Griff bekommen. Weil eben, du sagst dann, «ja scheisse, ich finde es nicht so toll, dass ihr diese zusätzliche Sicherheitsfunktion nicht eingebaut habt, aber das Gerät ist so geil ich kaufe es trotzdem.» Das heisst, man hat es offenbar geschafft den Leuten das so unter-schwellig als "nicht so tragisch", "vertrau uns doch", und "das ist eh das Coolste" zu verkaufen, das wir einfach sagen: "Oh ja, muss ich kaufen". Das heisst aber nicht, dass Privatsphäre, Persönlichkeitsrecht als solches nicht mehr gültig ist. Man sagt ja oft: «die Jungen interessiert es nicht, die posten ja jeden Scheiss.» Das ist ein Teil davon, also ein Unwissen. Wenn du ihnen aber erklärst was alles passieren kann und auch ein Beispiel zeigst. Einige sind dann schockiert und andere interessiert es dann nicht. Aber Solchen wäre es vermutlich auch schon vor zwanzig Jahren egal gewesen. Damals hatte es diese Instrumente einfach noch nicht. Heute haben sie diese Kanäle und wir haben es verpasst den Umgang so zu kanalisieren und kontrollieren, dass man sagen könnte "hey, du kannst es schon brauchen, aber pass auf". Also, der Zug, dass man vorbeugend dafür sorgen könnte, dass keine Data Breaches, kein Vorfall passiert, dieser Zug ist abgefahren. Ich meine diese Daten sind effektiv überall. Alles wäre mir ja egal wenn ich wüsste und eine quasi Leine hätte, damit ich wüsste, auch wenn meine Daten auf dem Amazon Server sind, ich habe jeder Zeit Kontrolle über Sie. Ich kann morgen Aufstehen und sagen: "Amazon, das wars mit uns, gib mir Alles". So, das könnte ich dann auch tun, Stecker raus ziehen. Aber heute ist das noch nicht möglich, weil Daten diese Eigenschaften nicht aufweisen. Diese Objektierung, diese Kapselung. Das wäre aber eine ideale Lösung.

Dir sind diese Eingriffe der Unternehmen bewusst, hast du selber auch einen Facebook Account?

U: Viele Fragen mich, "ja, sie, wieso haben Sie denn überhaupt Facebook". Mein Ansatz ist dann, wie könnte ich das Thema überhaupt beurteilen wenn ich mich einfach ausschliesse. Ich poste aber z.B. nie was ich gerade am Morgen gemacht habe und ich mache das auch sehr bewusst. Ich habe ein Interesse zu verstehen, durch erleben, wie diese Medien funktionieren. Ich sehe das als meinen Job, für meinen Job.

Wir können es also nicht verhindern und wir haben noch keine möglichen Lösungen um es zu kontrollieren. In dieser Zwischenphase in der wir sind, wird es natürlich nach allen Regeln «der Kunst zu meinen Gunsten» ausgenutzt wenn ich in Amazon bin. Sie profitieren. Selbst wenn es technische Mittel gibt, solange niemand sie fördert, dann bauen wir sie auch noch nicht ein. Da muss man die Menschen packen und ihnen einen anderen Weg zeigen.

Nehmen wir ein normalen Menschen, wie viel weiss er wirklich über diese ganze Verknüpfungen und das Netzwerk?

U: Sehr wenig. Nein, das ist eben der Punkt. Die Aufklärung hat natürlich null bis gar nicht stattgefunden. Ich meine, ich mache das schon sehr viele Jahre und ein Thema das noch recht gut bei Kunden aufweist wie wenig sie davon wissen und verstehen sind solche 'Live-hacking Shows'. Da hacken Leute live ein Handy oder ein System. Damit sieht man, dass man so was auch innert 5 Minuten hacken kann, wenn man weiss wie.

Aber die gibt es schon ewig, diese Live-hackings. Ich habe die schon vor 10 Jahren gesehen, es gibt nichts Langweiligeres. Ich unterschätze wie viele das immer noch nicht alles verstehen oder gar keine Ahnung von diesem Zeug haben.

Ich begegne oft dem Problem, dass Unternehmen meinen, ich will ihnen das Leben erschweren indem wir diese Sicherheitsmassnahmen einsetzen. Aber Sicherheit sollte niemand stressen, es ist eine Eigenschaft. Mein Ziel ist es immer meinen Job so gut machen, dass du gar nicht merkst dass du sicher bist, aber du es bist. Sicherheit wollen alle, sie ist etwas schwer zu spezifizieren und du merkst es vor allem erst dann wenn du sie nicht hast.—

»Sicherheit wollen alle, sie ist etwas schwer zu spezifizieren und du merkst es vor allem erst dann wenn du sie nicht hast.«

D1dact1c Tr@nsf3r - X-pl0ring L1v3d Sp@ce

Introduction

So far I have outlined the current state of **digital technology** and the impact it has on ways of experiencing and being in the world, arguing that **hacking** is a method which can be used to subvert existing digital systems and networks. Hacking in this way helps us gain a better understanding of these systems. After this we may begin to engage with our technological devices in new ways, with the potential of emancipating ourselves from our current use of them. The process is then twofold: First we must explore their capabilities and limitations. Second, we begin to reveal their structural absurdities.

In recognizing these absurdities, which often blur standard notions, or binaries, there then exists a space which may lead to liberation.

This process ought to begin within the younger generations, as they will be the ones who dictate technology's future uses. They are also avid and active consumers of the technology we possess today.

These digital natives consume information through **social media** on a regular basis, and therefore education should lay value on teaching them responsible means of interaction.

Therefore, I will outline a possible project for aesthetic research that can be used to encourage self-reflection and educate teenagers on how we use technology today.

Aesthetic Research - What's that?

Aesthetic research can best be described as a process; it requires the use of different methods and strategies to work through or manipulate an area of interest or relevant investigation, connecting strategy (procedural knowledge) with theoretical/cerebral activity (conceptual knowledge) in a playful and explorative way. (Jansen 2000, pg.19)

There are many ways to initiate or approach aesthetic research, using for example: "a question, a thought, a feeling/sense, an object, a plant or animal, an artwork, a person (fictional or real), a fact or situation, a literary theme, a linguistic term, complex content or - really - anything else." (Jansen 2000, pg.19)

It is important that this activity and process be self-initiated and self-motivated by the student. The key is that these methods of approach are connected and impact each other in a comprehensible and traceable way. Helga Kämpf-Jansen additionally notes, that locations and daily experiences are particularly interesting physical and conceptual spaces for the initiation of aesthetic research and discovering a central concern.

Within the process of research, classical methods of artistic expression, e.g., painting, sketching, filming, modeling, sculpting, photography, computer-based imaging etc., offer methods that enable students to document experiences, ideas, feelings, questions or concerns. The collection of these documentations are subsequently handled using methods commonly used in scientific investigation, i.e., theoretical researching, probing, questioning, categorizing, archiving, organizing, comparing etc. Through both the collection and this investigative approach toward these materials that have been created, students will automatically be forced to self-reflect on their process. This self-reflection enables students to situate themselves within their central concern and develop a positioning toward their investigation. Aesthetic research, therefore, becomes a circular process of production and reflection on a central concern, which leads to the refinement of thoughts and recognition of autonomy and self-efficacy within a thematic discourse. Students learn to become self-sufficient agents, and encourage their own curiosity by exploring topic central to and meaningful in their lives. Helga Kämpf-Jansen confirms this stating, "Wem diese Möglichkeit gegeben sind, wird sein Leben anders leben -vielfältiger, interessierter, mit größeren persönlichen Gewinn und er/sie wir - in kunstpädagogischer Verantwortung - ... vom ersten Tag an ganz andere Erfahrungsräume erschließen."(Jansen 2000, pg.21) In other words, those who embark on aesthetic research open the door to a new perspective and way of engagement with the world around them.

The following project leads students through a possible field or setting for aesthetic research and is, therefore, best suited for students ages 13 - 16. While the project may be attempted with younger students, critical reflection must be more heavily guided by the teacher as it is key for their conceptual understanding of the investigation and is what ultimately encourages their own motivation and interest.

Students 16+ can also implement this project, however in this case one would immediately jump to Step 4. The older students require, and should be given, more autonomy in developing their own ideas for reflection and exploration.

Learning Objectives

- 1 To become familiar with methods of aesthetic exploration
- 2 Learn how to engage with material and environments in a reflective way
- 3 Understand the importance of reflection and self-reflection in process
- 4 Successfully organize thoughts and ideas into a project idea
- 5 Demonstrate organizational skill by executing the idea within the given time
- 6 To become more cognizant of how identity can be constructed and how digital media influences this
- 7 To demonstrate technical proficiency and use of media skills, both digital and physical (classical artistic)

Step 1

Tracking physicality in daily lived space (180 min + 1 week for the collection of information)

Instruct students to take note of their travel routes for a week. Students must keep track of the locations from which they depart and to which they arrive. Tracking can be through visual or written documentation, i.e., photography, sketching, collection of found objects, or scientific notation of experiences. Students should investigate their daily commuting patterns, by tracking how they geographically move about a specific location or area. As they are tracking, they should begin collecting their impressions in a methodical way; how this is done is up to the student, but it must be observable or presentable.

Input A

While students are doing this, ask them to research Artists such as: Hamish Fulton (all work), Julie Mehretu (all work), Guillermo Kuitca (all work), Kathy Pandergast, and Maya Lin (Blue Lake Pass), Richard Serra (Tilted Arc). The goal should be to observe how other artists have used mapping within their work, and discover why this interested them. Students have not yet been given the opportunity to set their own boundaries of investigation or define a central concern of their own. Therefore, by showing them other artists that have explored this area, "geographical location and bodily motion/interaction with space", students will hopefully find meaning and purpose in their need to track their commuting patterns.

Points of discussion: The role of location, found items, collage

Step 2

Ok Google, map that for me! (270 min)

Once students have kept track of their daily routes and paths during the week, ask students to gather their collected material. Once they have their collected material gather allow students 10 minutes to write about any potential gaps they might identify in their material, i.e., missing locations, missing photographs of key locations etc. Once they are finished, ask students to draw maps of their environments based on their collection of material.

After students have created their own maps to express their exploration of their encounters with their daily commutes and environments, give them a google map print out and ask them to draw lines of their commuting behavior between locations that they have identified as significant. These maps will likely show areas of concentration, which will signify hot-spots - areas of their most frequent interactions.

Ask students to then reflect on their maps and their hot-spots:

- What are the differences between the two maps?
- Why might these differences have occurred?
- What makes these places/locations important in their daily life?
- What types of interactions occur there? Have they documented on of these places on social media? If so why?
- What about the paths between the hot-spots, is there one more frequently used than others?
- What is experienced, or seen while following that path?

Students are encouraged to reflect on their physical interaction with their location, and initiate a dialogue with a classmate. Have students then journal about these reflections; allow up to 30min.

*Note: At this point technology has not been heavily used yet, in terms of its capabilities of tracking. So far, they have used it to document their process, but have not been made explicitly aware of other operational functions that may be running in the background as they are doing so. Therefore, initiate the discussion with students about how this process might relate to technology, and their use of specific **applications**, i.e., **Snapchat**, **Instagram**, **Facebook** etc. It should now be clear to students that they have been tracking their own physical motions, the same way that their **smartphones** do.*

After students have verbally reflected on these paths and hot-spots with a classmate or in groups, ask students to silently record their findings. Ask them to choose an aspect of what was discussed and begin to reflect more deeply on this in relation to particular location that is important to them or of interest. **For homework:** students should write about and give reasoning for their choice in their workbook.

Step 3

Let's Snap that! (90 min)

To start: Ask students to hand you their Homework, so that you can begin reading this while they discuss ideas in the following activity.

Most smartphones have a battery usage list; within this list you can see which applications are most frequently used, based on how much battery power they have consumed. Have the students list their top three **applications**. (Hopefully at least two of these will be social media related, i.e. either Snapchat, Facebook or Instagram.) See if there are any similarities in the class. If so, ask these students to group together in groups of 2 - 4. In these groups, have students reflect on what characteristics their chosen application has, thinking about what distinguishes it from others:

- Is video/film the main form of communication?
- Is it still images?
- Is it text?
- What types of interactions can be experienced using the app?
- What makes it more popular than other applications?
- What are some adjectives you would use to describe it?

Give students about 30 min to discuss this in groups and ask them to also give concrete examples of the differences, sketching or drawing their reflection. Once they have completed their analysis ask the groups to divide themselves, so that a new group is formed with a 'specialist' in each application. This new group should now discuss their respective apps and strengthen their understanding of the differences between each of the apps they focused on.

The goal is to get students to think about modes of digital communication. They should begin to understand how certain types of media encourage certain modes of engagement.

Step 4

Let's bring it all together, time to explore! (90 min)

Students should now have an understanding of their own interaction with their environment and how different media can contribute to different modes of engagement. The next step is to ask students to take their written reflection on their location of interest (which was a homework assignment), and re-acquaint themselves with that location. Using one of the applications that was investigated, they should now observe their chosen location through this perspective. Is it possible to find existing material? What must they search for? Is it a location that is unknown and requires they create digital content?

Students should spend a whole lesson looking for online material. It is important that they immerse themselves in the **digital space** of this location and do not return to physical interaction - at least for this step. If they can't find anything on that specific location, ask them to think about some of the features it has, and instead search keywords relating to that.

Step 5

Sourced Material = New Beginnings (12 h)

Students should now have a collection of digital material. Students should reflect on this material and make observations and connections to previous discussions. What is present in the form of this material? What kind of story does it tell about the location? How do they feel about the location from their interaction with the digital material vs. actually experiencing it? Is there anything missing about the location that perplexes them, as they find it to be integral of its identity?

Input B

During this class introduce the art historical context of cyberfeminism and post-cyberfeminism. Discuss with students how they might find themselves in the discussion, or perhaps how they might feel excluded from it. Focus on how it is a movement to re-contextualize identity and reclaim it amid static binary structures. Lead the conversation and ask them to reflect on how the contexts of their life define their own constructed identity. This exchange should take place together as a class. In order to tie this in effectively, it is important to express the role of social media in contextualized identities, not only of people but also of environments, or terminology (hash-tags). Have them think about the identity of the location they chose as a focal point and the reflections they had about its digital identity vs. its physical one.

After leading students through a series of methods through which they have accumulated material and knowledge about a specific location, it is now time to ask them to conceptualize a continuing project involving or leading from this material. Their use of media should not be limited, in fact, the utilization of at least two types of media should be encouraged.

Requirements

- **Must** be executable within the remaining 10.5h (Students might not know what this means initially, so it is your role to guide them through contextualizing this constraint and making them aware of time consuming aspects of their proposed process/project).
- **Must** in some way incorporate or reference and aspect - as discussed in class exercise - of social media, in an unexpected way.
- **The entire process of arriving at the idea** must be documented in written and visual form in their workbook.

Your aim is that they can in some way reclaim this location. Students used to passively experience this environment, and now they must re-engage with it somehow.

Input C

Artists that altered themselves – ORLAN & Neil Harbisson. This input is meant to highlight how technology can enable new perspectives. How will they use their research thus far to create or evoke new experiences within this location? So, not only can technology re-contextualize identity, but our use of technology as part of identity can enable a new method of expression and experience.

The goal is to give students a sense of agency within their daily encounters and make them aware of how to encounter the routine with a new perspective. In this sense they are hacking either the identity of the environment or their own identity within the environment. Sometimes, it might even be both.

References for Input B

Donna Haraway's essay A Cyborg Manifesto was the foundation for the cyber feminist movement in art (1980s to 1990s). This topic is important in order to highlight our current need to re-contextualize cultural norms. Some of the work can be very graphic, so it is best to do research of specific works to show students first (look instead to Roberta Breitmore and Faith Wilding). The most important part is that there recently has been a resurgence of Cyberfeminist perspectives, renamed: 'Post-Cyberfeminism' or Cyberfeminism 2.0. The perspective now is less about female empowerment, and instead about a global interest in restructuring systems powered by corporate and governmental interests.

Additional Reading on the Topic of being Cyborg

A Cyborg Manifesto – Donna Haraway

After the Future: n Hypotheses of Post-Cyber Feminism – Helen Hester

I listen to color – Neil Harbisson (TED Talk)

Gloss(0)vary 2.0

Computer Programming

The study of and ability to communicate with computers and steer their processes. This generally involves the knowledge of computer languages, which engineers have created over the years to abstract the flow of binary series into more comprehensible actions and commands. Computer languages include: *A – 0, FORTRAN, C++, Java, html, Javascript, Python, Ruby, etc.*

n. Programmed / v. Programming / adj. Programmable/

n. A digital device that operates because it uses a logic, which has been written in in a computer language, to determine its functions.

v. The ability to use computer languages to write these functions in computer language to control the operational abilities of digital devices.

adj. The capacity of a digital device to be operated through the use of functions as defined by a particular computer language.

n. Code / v. coding / adj. coded

n. The script of logic, containing functions, used to operate digital devices.

v. The ability to write the script for this logic. This generally involves understanding computer languages.

adj. When the logic of a digital device's operations have been scripted into computer language.

Computer Scientist

A person that is studying computer programming and has the capability to program the systems of digital devices. Over the years there have been many notable computer scientists; Grace Hopper was one of the early female voices in computer science. She discovered a moth between computer relay, effectively coining the term 'de-bugging' – the act of removing problems in the programmed logic so that the system can continue to function.

Feature engineer

A computer scientist that focuses on coding a program, that is using machine learning, to look for specific features in the data used to train the system. - [see also: **machine learning**]

Cyborg

A person that is at once human and machine(technology), with the ability to steer both of these systems digitally. There is one officially declared cyborg, Neil Harbisson, who has surgically altered his body to include technological systems. However, even the general public may find that we tend toward cyborg interactions with our electronics, by using technology to enhance biological behaviors and systems of communication.

[see also: **Technology, Digital, Cybernetics**]

Cyborg systems

Systems that are both mechanical(technological) and biological and ca be steered digitally

Cyborg identity

Our current identity as humans today; living in a society that symbiotically utilizes and implements the use of technological and biological systems, which can be steered digitally to alter ourselves and our environment.

Cyborg activist

Someone who encourages the rights of cyborgs and advocates the technological morphology of humans. (see www.cyborgfoundation.com for further information on how to become one yourself)

n.Cybernetics / adj. Cybernetic

n. The study of control and communication in animal and machine, with the ability to steer both these biological and technological systems in merging them through their interactions.

adj. This is when the control and communication in animal and machine has the capacity to be steered digitally through their merging interactions.

Cybernetic systems

Systems of control and communication in both animal and machine that have been merged to enable digital steering.

Cyberspace

A colloquial term to describe the space in which computer communication occurs.

Databanks – i.e., storage of data

The location of data storage, generally on remote servers that are physically consuming electrical power to execute this function.

Data sets – i.e., actual data

A collection of data, generally part of a single database (collection type). This data can either be discrete, i.e., numerical values, or categories – like male, or female – or it can be continuous, i.e., a measured value that could include a possible range.

n. Digital/ adj. digitally

n. A signal expressed as a set of binary series, represented by 0 (false) or 1 (true) which often has a physical correlation to electromagnetic output or voltage. In this sense, all our devices, which contain a chip use digital means to in order to function. Using these binary series is what allows one to steer what is digital.

adj. This is when a signal is expressed in a set of binary series

Digital information

Information obtained through the use of digital devices, such as; computers, smartphones etc.

Digital device

Devices that operate through the correlation between binary series and electromagnetic output or voltage.

(**syn:** digital technology) - see also: [**digital devices** under **hardware**]

MAC Address

MAC - media access control address - is a unique identifier of all forms of digital devices, particular to that piece of hardware. - see also: [**hardware**]

Digital mobile devices

Mobile devices that operate through the correlation between binary series and electromagnetic output or voltage.

Examples include: Smartphones, iPads, e-Readers, Laptops, Smartwatches, and Fitness trackers

n. Digital networks / adj. digitally networked

n. System networks that correspond in order to execute tasks and functions based on sent and received binary series.

adj. when something is connected through a network that corresponds through sets of binary series

Digital platforms

Programs and systems built on the logic of binary series and operations.

Digital space

The space created through the transmission of binary series between devices. A colloquial term often used to describe in general the systems we use as pertaining to various technologies.

Digital technology

Machines that operate through the correlation between binary series and electromagnetic output or voltage.

(**syn:** digital device)

Digital technology's vortex

Our current malaise of being consumed by the production of digital media through the use of digital technology, which we then ironically proceed to consume. This can be understood to be for personal production, corporate production or entertainment production.

Ergonomic gestures

Physical motions that correlate to [map on to] actions that have been programmed in a digital device. For example: swiping up or down to scroll a page, expanding two fingers in a pulling-apart motion to zoom in on an image, swiping to the side of a screen to dismiss an object.

Hardware

The physical parts or components of digital devices/digital technology, such as: the monitor, the computer's data storage; often a hard-drive, a physical server, or graphics cards, etc.

MEMS microphone

MEMS stands for Microelectro-Mechanical System. MEMS microphones are therefore small electronic mechanical microphone systems. They are often found in digital mobile devices.

Un-wired vs. wired

All digital technology requires power to run, this power is generally obtained from electrical wiring, i.e., wired. When the power required to run digital devices decreased and the power of battery components increased, due to developments in the production of their electrical mechanics, they became battery operated. These developments led to *mobile* digital devices that could be easily transported and carried, i.e., were un-wired.

Digital devices

A collection of different pieces of hardware that operate in unison between binary series and electromagnetic output or voltage. - see also: [digital devices under digital]

Smartphones

Digital mobile devices that can be carried around easily, due to their small size. Mostly, smartphones have a touchscreen that allows interaction with the interface and system of the device through physical touch and motions.

iPhone

A smartphone produced by Apple. iPhones are widely popular for their ease of use and style. However, the native applications are not always the best, and they do not allow for a lot of user customization. Plus, their glass screens are a constant source of concern, as they break easily – even with a case and a thin sheet of protection glass.

Blue box

A small device that grew popular in the 1970s, that could transmit specific frequencies, and were connected to telephone lines in order to circumvent the tolls on phone calls that were collected by telecommunication companies.

Home listening device

A digital device that can be activated with voice commands, and can be linked to other technology in the household, with the general purpose of organizing these processes, such as: playing music, giving, turning on the lights, letting you know when the laundry is done, etc.

Alexa

Amazon's home listening device, other than being able to execute standard functions, such as playing music, Alexa can also purchase items from Amazon. There is also the option to program Alexa with personal purposes and corresponding output responses. But, be careful, if your toddler starts talking about castles, you might just receive that doll house they wanted the next day. She also had a bit of a break down last month and began creepily laughing for no apparent reason.

Plug & play

This is when a device requires little or no prior knowledge for the user to begin using it.

v. Hacking / n. Hacker

v. Hacking is the subversive behavior of exploring computer systems, networks and digital devices, by playing around with their functions to discover vulnerabilities or problems in them which can be used and re-contextualized way.

n. Someone who explores computer systems, networks and digital devices by playing around with their functions in order to discover vulnerabilities or problems in them which can be used in a re-contextualized way.

v. phreaking/ adj. 'phreaking'

v. The hacking of telecommunication lines. Generally made popular in 1970's thanks to an article by Ron Rosenbaum in Esquire Magazine.

adj. Although this may not be how the terminology originated, "*phreaking*", aka. "*freakin*", is a form of expressing emphatic amusement/amazement or alternatively extensive frustration - so perhaps there is a link after all.

Internet/World Wide Web

A globally connected computer network that provides a large amount of information, and various communication abilities, through interconnected networks using standardized protocols of transmitting the data. The internet first came online, known as the World Wide Web in 1990 [this is what the www. Stands for in a URL]. URLs are used to contact webpages as hyperlinks.

Public Domain

A global copyright standard that insures the authenticity and security of creative work and property. In 'tech', it mostly refers to public websites that are reachable through the internet and do not require any additional security permissions.

Servers

A computing device that provides the functionality for all other programs or digital devices and manages the access to centralized resources or services in the network. These other devices are referred to as *clients*.

Remote servers

A computing device that provides the functionality for all other programs or digital devices and manages the access to centralized resources or services in the network, and is not close in location to the client. Unless you work within a company where the servers are present within the same office space or building as the computers connected to it, most servers end up being remote to the clients using them.

Web search

When using the internet you can use search engines to look for specific information. This process is referred to as a web search.

Webpage/Website

This is an interactive page on the internet, generally with different layers which are linked together.

Webserver

A server that uses a html protocol and thereby is also connected to an internet network.

Differential privacy

A method that aggregates data from personal users into a more general pool of data in order to secure the individuals privacy. So, instead of creating data directly from a single user, the system codes user preferences and in a sense takes count of these decisions or behaviors, instead of collecting the raw data itself.

Cryptographic algorithm

An algorithm, written to randomize numbers, in order to create encryption keys. In this sense, random is not complete randomness. However, unless you have the algorithm by which randomization was created, you will not be able to crack the code.

Keychain

There are different processes in computers that set up the system and monitor the inputs used for secure access. The memory of these passwords is called the keychain. There are several web services and other software programs that enable users to store their passwords securely. (Well, at least we hope they do.)

DHCP

The Dynamic Host Configuration Protocol manages the network connection by processing other protocols and assigning IP addresses in order to enable communication in the network.

IP address

These are unique identifiers during a network connection/session. IP addresses, however, are not unique to the devices that use them. They can instead be thought of a range of possible identifications that can be used within one network to communicate with another. When you connect through your internet at home, your service provider owns a range of IP addresses, and your device locates an available one within your network in order to then communicate with others.

DNS

The Domain Name System is a protocol that assigns website domains to IP addresses so that they can be contacted by a computer. So perhaps www.example.com would correspond to: 70.42.271.42

HTTP/HTTPS

The Hypertext Transfer Protocol is a protocol used for the internet to distribute collaborative media channels and systems.

TLS

The transport layer security is a cryptographic protocol and acts as an additional layer of security to maintain a safe connection between devices.

Query

When a device requests something from another system.

TCP

One of two general methods of routing information through – generally internet based – network connections. TCP requires all the elements of necessary information to be read and considers any missing gaps in the transfer. If this occurs the TCP protocol will post a query to ask for this missing information to be sent again, only after receiving all the parts will it display the information received. It's like if a waiter brought you coffee without a cup to pour it into.

UDP

The second of two general methods of routing information. UDP unlike TCP will process information as it arrives at the receiving end, it will not additionally post any requests to the source. This would be like your waiter showing up with your ordered piece of cake - even if you don't have a plate or any silverware, you can still eat it. Although, it might not be graceful, it is possible!

Man in the Middle Hack

This is when someone is able to make it appear as if you are connected to a secure and safe site, when in fact you are connected to their machine that is mimicking it. Remember all those action films, in which they freeze the security cameras - and no one has a clue about what is really going on behind the frozen screen? Well, the man in the middle attack is exactly like this.

Certificates

Just like other certificates, these certificates confirm the authenticity of provided 'work' – in this case they identify a authentic website.

Telecommunications overlay network

A telecommunications network that is connected within an internet network, but is in a way compartmentalized or structured on top - laid over - of the base internet network.

Signaling systems

Systems that can transmit different frequency signals through the use of binary series.

Machine learning

The study of creating systems and software that can learn from data sets, making sense of their significance, in order to progressively improve their functions. Based on the initial programming and identification of relevant features in the data, these systems then determine what kind of features should be considered in subsequent analyses of the data in order to achieve better results. Initially the data's features must be determined by a feature engineer (see feature engineer).

Neural networks (neural nets)

Programs whose architecture simulates processes of the human brain, in order to generate software that can learn from data independently and set its own features and functions in order to achieve progressively better responses.

Mainframe

A computer that is often used by large corporations or organizations to process large quantities of data, or run critical applications, and used as the main location of storage. It's what all those action heroes try to break into in action films.

Social Media

Social media is used to communicate digitally with other people. This can be in an individual sense, through private messaging, or through more public formats that allow others to interact with or view your profile and media, which generally includes: short videos, photographs or text.

Facebook

This is a social media platform that allows you to connect with friends, and post information from websites, videos or images on their profiles - or *walls*. In order to connect with others, you must grant them permission to become your *friend* on the application. Facebook contains its own messaging layer, which has the option of calling or video calling your connections. (For more information, just watch *The Social Network*, or even better, read the news!)

YouTube

This is a social media platform that allows you to upload videos. Users have their own feeds and playlists you can follow. Lots of news providers and comedians may have their own channels. Those who use YouTube to blog (record daily life are referred to as "Vloggers" - video bloggers. You can essentially learn how to do almost anything through YouTube videos. Want to play the guitar, check out YouTube. Want to build a cabinet set, check out YouTube.

Instagram

This social media platform allows you to share images through your profile. There is now the option to create 'stories' – short snippets of (generally live) video footage – that give your followers an insight into your daily life.

Snapchat

Snapchat is similar to Instagram in many ways. They were the first to think of the concept of 'stories', as a live feed, to sharing your current activity or other interesting news. Initially the app was used to send naked pictures to others for the purpose of sexting – provocative sexual messaging between two individuals. Snapchat was used, because your sent messages are only available for a limited amount of time (up to 10 seconds). However, it is possible to take screenshots of these photos (although the other person is now notified of this activity on their end). In addition, in its early years, snapchat was hacked many times. Photos sent through the app were subsequently leaked online.

SMS messages

SMS stands for Short Service Message and is the standard text messaging component in digital mobile devices, which uses the internet to transmit them.

Software

A part of a computer system that can be programmed, constructed, and altered, using data from sets of binary series to process coded tasks and commands that the computer can then execute. (syn. Program)

Application / app

A piece of software that is designed to fulfill a particular task.

Native application

An application that was built to run within a particular operating system.

Interface / pl. interfaces

The communication through which software and hardware, or other peripheral devices communicate. In general use the interface refers to the visual space within the system that has been programmed to appear through a monitor, and allows users to control the system.

Graphical user interfaces (GUIs)

These interfaces always have a visual component and are what allow us to control, and communicate with, our digital devices. It makes navigating webpages or other software a simpler task, by abstracting the code it has been built upon into visual layers that produce immediate feedback. For example, when I click a button such as the 'save' icon, to save my document, a window pops open.

User-friendly interfaces

Interfaces that have been designed to enable ease of use.

CGI Computer Generated Imagery

Images created using computer programs and algorithms.

Artificial intelligence

Software that is built with the intent to imitate human cognition. Some famous systems include: Siri, Alexa, IBM's Watson, Kiva – amazon warehouse robots etc.

Digital Assistant

Generally this is some form of artificial intelligence that caters to user preferences. It's like having a real assistant, but without the cost. However this comes with the compromise, that *she* also won't possess the ability to grab you a real cup of coffee when you ask for one.

Digital voice assistant

This is a digital assistant that can understand natural language - your spoken requests. *She* will also answer you verbally and conduct all communication through vocal cues. Popular digital voice assistants include: Siri, Alexa, Ok Google, Cortana. (Generally the default programming consists of a female voice)

v. Parsing

The analysis of syntax – generally speech – into logical commands that can be executed by the program or software.

Siri

This is Apple's digital voice assistant. You can ask her lots of different questions, and she is an almost endless resource of fun when you get bored. Just as her what her favorite pick-up line is; she might have a few good ones for you...

Technology

The instruments we create in order to aid our execution of tasks and processes. In this text, technology refers to the electronic systems, computers and digital devices/digital technology that we use.

Relay computers

Relay computers were computers that used electromagnetic switches to execute functions. Whether the switch was on or off determined if a 1 or 0 was written into the set of binary series.

Computing

The use of computers to complete tasks.

Computing power/Processing power

The speed at which a computer, program or system can process information.

Technological vulnerabilities

So, you know that one family member of yours, that cyborg who doesn't really like their teeth, their V5 Eye sockets, or the fact that their gait is slightly off due to their latest system upgrade?

We've all just about heard enough about their insecurities and their vulnerabilities. Technological systems also have weaknesses and sensitive areas, that when exposed become critical and dangerous vulnerabilities.

Generally, hackers take advantage of them and use them to their own advantage. So, that cyborg with the limp - try stealing their purse, with that limp they won't be able to run after you as quickly as you might think.

Operating system

The base code that runs on digital devices and enables them to process data sets and information, enabling them to operate.

Virus/pl. viruses

If you get the flu, you generally start to become sluggish. You may lay in bed all day or have other adverse symptoms, such as: coughing, sneezing, shivers, etc. The flu is caused by a virus. When your digital device becomes infected by a digital virus, it may begin run more slowly or encounter problems that lead to adverse symptoms, such as: shutting down unexpectedly, overwriting file data, etc., in the same way.

Digital Native

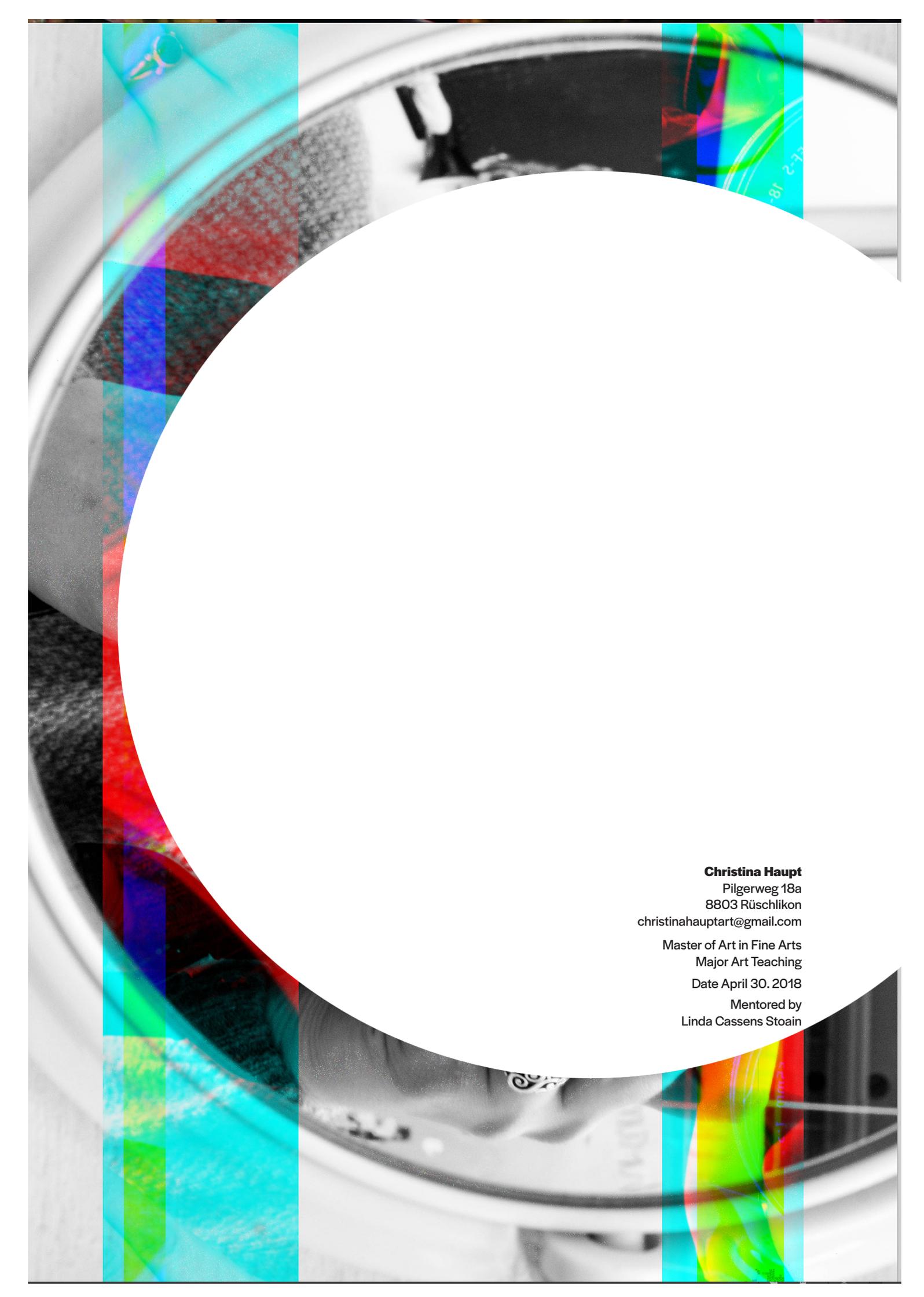
These individuals include those who have grown up with digital devices around them their entire life. They might remember the times of hop-sotch and tag, and find themselves still draw to the outdoors, but they understand the power behind computing, and are able to use it as if it were an extension of the body and mind. Thinking about it now, I guess digital natives are really just all of us cyborgs.

Bibliography & Works Cited

- Alepis, E., & Patsakis, C. (2017). Monkey Says, Monkey Does: Security and Privacy on Voice Assistants. *IEEE Access*, 5, 17841–17851. <https://doi.org/10.1109/ACCESS.2017.2747626>
- Anderson, Cristen. (2018) Personal interview with Cristen Anderson
- Anderson, Monica. (2016). More Americans using smartphones for getting directions, streaming TV [Data Analysis]. Retrieved from <http://www.pewresearch.org/fact-tank/2016/01/29/us-smart-phone-use/>
- Arnold, Michael. (2003). On the phenomenology of technology: the “Janus-faces” of mobile phones. *Information and Organization*, 13(4), 231–256.
- Computer History Museum. (2018). Timeline of Computer History [Organization]. Retrieved March 25, 2018, from <http://www.computerhistory.org/timeline/1985/>
- Dörig, Raffael. (2014). Hacking Everyday Life. In *Hacking Edition Digital Culture 2* (p. 269). Basel: Christoph Merian Verlag.
- Elbaor, Caroline. (2017, November). What Is Post_Cyberfeminism? Here’s a Primer on the Latest Big Idea to Storm Contemporary Art. Retrieved from <https://news.artnet.com/art-world/an-introduction-to-post-cyberfeminism-1156271>
- Haraway, D. J. (1991). A Cyborg Manifesto. In *Simians, cyborgs, and women: the reinvention of nature* (pp. 149-181pp.). New York: Routledge.
- Heidegger, Martin. (1977). The Question Concerning Technology. In William Lovitt (Ed.), *Technology and Other Essays*. New York: Harper and Row.
- Herman, Laura M. (n.d.). Synesthesia. In *Encyclopedia Britannica*.
- Hester, Helen. (2018, January). After the Future: n Hypotheses of Post-Cyber Feminism. Retrieved from <http://beingres.org/2017/06/30/afterthefuture-helenhester/>
- Jeffries, Stuart. (2009, January 7). Orlan’s art of sex and surgery. *The Guardian*. Retrieved from <https://www.theguardian.com/artanddesign/2009/jul/01/orlan-performance-artist-carnal-art>
- Jeffries, Stuart. (2014, June 5). Interview: Niel Harbisson: the world’s first cyborg artist. *The Guardian*. Retrieved from <https://www.theguardian.com/artanddesign/2014/may/06/neil-harbisson-worlds-first-cyborg-artist>
- Junker, P. & Molyndris, N. (2018, September 3). Personal interview with Nikolas Molyndris and Philip Junker.
- Kämpf-Jansen, Helga. 2000. *Ästhetische Forschung. Wege Durch Alltag Kunst Und Wissenschaft - Zu Einem Innovativen Konzept Ästhetischer Bildung*. Köln: Salon Verlag.
- Kämpf-Jansen, Helga. 2012. *Ästhetische Forschung*. Marburg.
- Kunzru, Hari. (1997, February 1). You Are Cyborg. Retrieved from <https://www.wired.com/1997/02/ffharaway/>
- Landwher, Dominik (Ed.). (2014). *Hacking Edition Digital Culture 2*. Basel: Christoph Merian Verlag.
- Mambretti, Andrea. (2018, November 3). Personal interview with Andrea Mambretti.

- McCarthy, John. (2017). What is Artificial Intelligence. Computer Science Department at Stanford University. Retrieved from <chrome-extension://oemmndcbldboiebfnladdacbfdmadadm/file:///Users/christina/Downloads/whatisai.pdf>
- McDowell, John. (1994). *Mind and World: with a new introduction*. Cambridge, MA: Harvard University Press.
- McLaughlin, Elliott C.. (2017, April 26). Suspect OKs Amazon to hand over Echo recordings in murder case. CNN. Retrieved from <https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html>
- Mozur, Paul. (2018, April 1). Internet Users in China Expect to Be Tracked. Now, They Want Privacy. The New York Times. Retrieved from <https://www.nytimes.com/2018/01/04/business/china-alibaba-privacy.html>
- Oral History Office. (2001). *Transcribing, Editing and Processing Guidelines*. Minnesota Historical Society.
- Petty, Felix. (2018). what we can learn about the cult of insta-influencers from lil miquela.
- Pias, Claus. (2014). Cultural History of Hacking. In *Hacking Edition Digital Culture 2* (p. 269). Basel: Christoph Merian Verlag.
- Quinto, Anne. (2016). This woman, a self-described cyborg, can sense every earthquake in real time. Retrieved from <https://qz.com/677218/this-woman-a-self-described-cyborg-can-sense-every-earthquake-in-real-time/>
- Rosenbaum, Ron. (1971). Secrets of the Little Blue Box. *Esquire*, 117–125, 222–226.
- Sadun, Erica. & Sande, Steve. (2014). *Talking to Siri: Mastering the Language of Apple's Intelligent Assistant* (3rd ed.). Indianapolis: QUE.EUGDPR.org. (2004).
- Sayej, Nadja. (2016, January 16). Interview: ORLAN: "I walked a long way for women." *The Guardian*. Retrieved from <https://www.theguardian.com/artanddesign/2016/jan/15/orlan-i-walked-a-long-way-for-women>
- Scott, Izabella. (2016, August 13). A Brief History of Cyberfeminism. Retrieved from <https://www.artsy.net/article/artsy-editorial-how-the-cyberfeminists-worked-to-liberate-women-through-the-internet>
- Smith, K.K. & Berg, D.N. (1988). *Paradoxes of group life*. San Francisco: Jossey-Bass Publishers.
- Song, L., & Mittal, P. (2017). Inaudible voice commands. *ArXiv Preprint ArXiv:1708.07238*.
- Strong, Tom. (2005). Review of Samuel Todes' *Body and World*. *Janue Head*, 7(2), 516–522.
- Todes, Samuel. (2001). *Body and World*. Cambridge, MA: MIT Press.
- Umberto Anino. (2018, July 3). Personal interview with Umberto Anino.
- Weaver, A., & Newell, N. A. (1954). In-Band Single-Frequency Signaling. *Bell Labs Technical Journal*, 33(6), 1309–1330.
- Wiener, Norbert. (1961). *Cybernetics: Or Control and Communication in the Animal and Machine* (2nd revised ed.). Cambridge, MA: MIT Press.
- Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., & Xu, W. (2017). *DolphinAttack: Inaudible Voice Commands* (pp. 103–117). ACM Press. <https://doi.org/10.1145/3133956.3134052>





Christina Haupt

Pilgerweg 18a
8803 Rüslikon
christinahauptart@gmail.com

Master of Art in Fine Arts
Major Art Teaching

Date April 30, 2018

Mentored by
Linda Cassens Stoain