AMRO Research Lab 2015 – servus.at

B E H I N D
T H E
S M A R T
W O R L D

Saving, deleting and resurfacing data

Edited by Linda Kronman and Andreas Zingerle

Published 2015 by servus.at
Kirchengasse 4,
4040 Linz
AUSTRIA

ISBN: 978-3-9504200-0-5

AMRO Research Lab 2015

This publication documents the first research lab[1] in conjunction with the Austrian net culture initiative servus.at based in Linz. The idea for this kind of lab, which is able to explore a specific topic and the associated challenges for the information age in depth over the course of one year, is rooted in the festival "Art Meets Radical Openness"[2], which takes place biennially since 2008 in cooperation with the Art University Linz. This is a community festival originating in the Free Software movement and the early Austrian initiative Linuxwochen (Linux Weeks[3]), but this event has been expanded with cultural, artistic, and social-critical aspects in connection with technology. When art meets radical openness, this suggests a paradox.

For what is generally considered contemporary art is rarely "radically open" in the sense that its authors purposely make sources, processes and contents accessible for further processing, as is the rule with F/LOSS (free/libre Open Source Software) projects. What may succeed in the development of free software, however, poses a challenge to us in the way we deal with information. Which information is meaningful and should be made accessible to whom in which form?

---

1 http://research.radical-openness.org/2015
2 http://www.radical-openness.org
3 http://liwoli.at (LinuxWochenLinz)

The festival brings together a diverse group of actors (artists, cultural workers, philosophers, software developers, hacktivists, activists, and journalists), who often operate in different fields at the same time (art, education, journalism, activism, software development and more) and principally agree on the value of using alternative tools, based on a social-critical stance. This fundamental stance influences not only how we deal with technology per se, but also the approach to issues concerning the complex conditions of our digital infosphere, which impels an unremitting cultural transformation that has a real impact on our life and the way we deal with our world today.

For us, the collaboration with the artist collective KairUs – Linda Kronman & Andreas Zingerle has proved to be very valuable. Their research topic “Behind the Smart World” with its original starting point of twenty-two harddisks from the largest recycling center in Ghana has led us to a collection of theoretical and artistic positions focusing on a fundamental problem of our times, the saving, deleting and resurfacing of information.

Us(c)hi Reiter – servus.at

Linz, November 2015

save

delete

resurface

'Behind the Smart World' - Introduction 7
by KairUs - Linda Kronman and Andreas Zingerle

If not us, who stores and owns our data? 16
by Fieke Jansen, Tactical Tech

Center of Doubt 27
by Ivar Veermäe

THE GOOGLE TRILOGY. 41
Or how to play with Google Street View in different ways
by Emilio Vavarella

Surveillance, McLuhan, and the Social Prosthesis: 53
Examining the Construction and Presentation of Identity
by Leo Selvaggio

What remains? The way we save ourselves 62
by Marloes de Valk

Times of Waste 71
by Research Team "Times of Waste"

Digital Data Funerals 83
Interview with Audrey Samson by Linda Kronman

Technology-based Art and Destruction - 93
Exhibiting Malfunctions
by Stefan Tiefengraber

Third Person Data 102
by Dr. Michael Sonntag

Behind the Smart World ArtLab – 121
artistic strategies for dealing with resurfacing data
by KairUs - Linda Kronman and Andreas Zingerle

Deleted file information is like a fossil... 133
Interview with Michaela Lakova by Andreas Zingerle

Strategies of Net-activists Against 143
Phishing and Fake Business Websites
by KairUs - Linda Kronman and Andreas Zingerle

COLOPHON 154 KEYWORD INDEX 156

‘Behind the Smart World’ – Introduction

The smart world. Created by policymakers, the advertising world, creative industries, and persuasive UX-designers that portray to us a world of shiny brand new technologies, apps that solve all our daily problems and smart cities collecting big data that will eventually solve all the problems of human kind. If we take a slightly more critical look at our smart world, though, our shiny gadgets become obsolete faster than ever, turning into toxic e-waste; our apps and smart cities have turned into an effective all-encompassing surveillance apparatus, and we have no idea who is collecting our data, who accesses it, and where it is stored. There may be issues that the smart world can solve, but at the same time, it raises new problems concerning data breaches, data privacy, data ownership and electronic waste. In this publication researchers and artists unfold some of these issues in three parts: Saving Data, Deleting Data and Resurfacing Data. Each part begins with theoretical texts that address some of the concerns, followed by strategies of artists and activists that expose problematic power structures, creatively reveal how we lost control of our data and offer strategies to deal with our data in this smart world.

Part 1: Saving Data

Ctrl-S / Cmd-S, saving our data used to be a conscious act, and we still use this key combination relatively often. When we use our smart phones, computers, tablets or other devices connected to the Internet, our data is increasingly saved without us realizing it. Programs have auto save functions, apps are so user friendly that they spread our data into the celestial clouds, and increasingly our behavior is tracked and saved by unknown third parties. In which ways is our data collected and saved? Is there any way we can know who is collecting our data, where it is saved and what it is used for? Fieke Jansen, researcher at the 'Politics of Data' program at 'Tactical Tech' writes about the blooming industry of data brokers who track us, collecting our data to create profiles of us that can be sold to those who persuasively lure us to become better consumers. She also offers some practical tips on how to avoid being tracked. Artist Ivar Veermäe continues to elaborate the topic of commercial cloud computing by questioning the rhetorics of IT companies who intentionally ignore the gap between immaterial information and the material architecture supporting it. Data-centers and their supporting formations are the focus of his long-term artistic research project *Center of Doubt*. Emilio Vavarella suggests metamorphosis as the 'essential goal of survival achieved through countless creative endeavors' as a strategy to resist technological powers. He

illustrates how he plays with the errors of Google Street View in a series of artworks assembled as *THE GOOGLE TRILOGY*. Obfuscation as a strategy to resist the apparatus that is constantly tracking us is offered by artist Leo Selvaggio, who reflects on the problematic issue of facial recognition in surveillance. Leo's *URME Surveillance* project gives the public a chance to hide behind a 3D prosthetic of his face. When Leo's faces appear in several locations at the same time, the ability to identify people through facial recognition systems is questioned. Even if this strategy might be rather problematic in the long run, it reveals yet another way in which our data is continuously saved by others, in this case as images, locations and times, waiting to be connected to the rest of our profile.

Part 2: Deleting Data

The second part of this publication still continues to reflect on 'the way we save ourselves'. Writer and artist Marloes de Valk asks: What will remain of our compulsive fetish of saving everything? In her article the consequences of saving data without the ability to delete it start to unfold. She describes some effects of our 'information-hungry lifestyles', such as the toxic lakes in China and e-waste dumped in developing countries. The article from the research team "Times of Waste" continues on the topic

of e-waste, focusing especially on recycle and reuse paths of smart-phones. What happens to our old phones, when upgrade to yet another model? When our electronics start their journey as waste for us, they might still be of use for others. Before we drop our smart-phone in the recycle bin or sell our computer parts online, we might want to delete the data on them. In Audrey Samson's interview we learn that deleting data is far more complicated than emptying the trash bin or resetting our phones to factory presets. In her works data is deleted by physically destroying the storage medium or concealing it, making it impossible to access. Destruction is the only 100% effective way of data erasure. Data recovery takes time, requires expertise and spare parts, but it has been proven possible in many cases. Though Audrey's artworks are symbolic 'data funerals', she also brings forth the problem of deleting data online. She explains some of the current policies for how online profiles are managed in case of a person's death. Once our data is uploaded to a server in the cloud, we loose ownership of it; while we are not able to access it, we are also not able to delete or destroy it. Stefan Tiefengraber's artworks also deal with the materiality of servers in data centers using destruction, while emphasizing how limited our access to them is at the same time. In his artwork *User Generated Server Destruction* visitors to a website have the rare opportunity to physically damage the server on which the website is hosted. The website goes off-line when the hammers installed on the

server take their toll on it. The works by Audrey and Stefan reveal that the ‘death of data’ leaves a material corpse behind. A rather toxic corpse, in fact, that does not decay easily, containing rare minerals and chemicals, some even valuable to mine. This ‘urban mining’ can be an effective way of reusing materials, but it can also be a health hazard and an ecological disaster when not done properly. The essays in this chapter connect the seemingly immaterial information, the ones and zeros of our data, to their material containers. Whereas the cloud suggests an unlimited capacity of storage space, one wonders where do the data centers go to die?

Part 3: Resurfacing Data

As the prior parts of the publication show, we live in a time when everything is saved, and this data is very hard to delete. When we share our data online, it often ends up being backed-up, duplicated, shared further and sold for profit. Traces of our data can therefore resurface in a number of places, as is made clear in the article by computer forensic expert Dr. Michael Sonntag, who writes about third person data, data that is collected and stored with our unwitting consent. He also outlines what personal data of ours exists and in which context it can resurface. We also carry an increasing number of items on us that store personal data. Do we make

efforts to delete the data on an old mobile phone before we hand it in for recycling, what about an old computer hard-drive, one that we might not be able to boot any more? What if we delete the data on the hard-drive, but it is not actually deleted? As discussed in the previous chapter, data is only effectively deleted if it is physically destroyed. But there are a lot of 'zombie hard-drives' resurfacing at flea markets, in containers shipped as donations to developing countries or at e-waste dumps. Which data resurfaces? Can it be re-used or abused? These were some of the initial questions we had when we bought 22 hard drives in Ghana at one of the biggest e-waste dumps in the world. The essay *Behind the Smart World ArtLab – artistic strategies to deal with resurfacing data* recounts the journey of these hard drives and how artists in an ArtLab dealt creatively with the data on them. Most of the data on such hard drives is information junk, waste of its own kind, yet personal data on these hard-drives raise a lot of ethical questions: Who owns the data? Can the data be (ab)used? Are we invading people's privacy just by looking at the data? Artist Michaela Lakova invites the audience to deal with these ethical questions in her installation *DEL?No,wait!REW*. In this installation data is recovered from hard drives bought from flea markets, and the visitor is confronted with the dilemma of either deleting the file forever or posting it on the Internet. In addition to this, Michaela explains about her other projects concerning the recovery of data and storage

mediums. Data is saved, duplicated, cloned, shared and published for different motives. Most of us would agree that spam mails and fake websites used for fraud should be categorized as the junk of Internet traffic. It is estimated that fake websites make up around 20% of the entire World Wide Web, and they are often clones and copies of sites published elsewhere. This type of resurfacing data is the focus of the last article *Strategies of Net-activists Against Phishing and Fake Business Websites*, in which we illustrate how open source intelligence tools can be used to report websites suspected for fraud and eventually have them blocked by their hosting providers. Nevertheless, when one domain is blocked, the same website often resurfaces under yet another slightly different domain name. This phenomena is also clearly visible in the artwork *Megacorp.* that visualizes a collection of 1000 fake companies.

KairUs – Linda Kronman and Andreas Zingerle


SAVI
NGDA
TA

If not us, who stores and owns our data?

by Fieke Jansen, Tactical Tech

In October 2015 the European Court of Justice ruled that the Safe Harbor agreement was invalid. This agreement enabled American companies that comply with European data protection law to transfer and store data of European citizens. Under the American Patriot Act this allowed US authorities to gain routine access to the online data of Europeans stored with American companies, which according to the European Court infringed on the privacy of EU citizens.[1] These jurisdictional issues around data stem from the fact that individuals no longer own or store their data, that third parties have become the data holders. The question we try to answer in this article is how do we lose control of our own data, where is it saved if it is no longer in our immediate surroundings, and what can be done to reclaim some control over our data?

---

[1] Powles, J. Tech companies like Facebook not above the law, says Max Schrems http://www.theguardian.com/technology/2015/oct/09/facebook-data-privacy-max-schrems-european-court-of-justice

How do we loose control over our data?

Our devices – computers, mobile phones, and tablets – are constantly telling others where we are and what we are doing. Mobile phones in particular are very effective tracking devices: Where we go, it goes, and it records our location all the time – even when we're not connected to the Internet. It also collects information about our contacts, which websites we visit, and the apps we use.

This might sound abstract, so lets take a closer look at location data. Location collected over time can tell a surprisingly full story about who we are and what our life looks like. Location data can predict where we live and work by analyzing where our phone sleeps at night and rests during the day.[2] Subsequently, if location data is layered with other data like Google maps, a company that has access to location data can tell where we have been: whether we visited the doctor, which restaurants we have visited frequently, and even whether we are part of a political organization. When location data is layered with time and data, the location can be linked to public events, which can tell something about participation in protests, the attendance of a concert or festival or even a visit to specific support group. Now imagine a company has access not only to our own location data, but also to that of all our friends and family. Putting these locations together can give insight into who was in a room together at what time, and from this social graphs[3] are built to identify what type of social relationships exist between people.

---

[2] Location tracking, Me and My Shadow https://myshadow.org/location-tracking

[3] Chatterjee, S. and Anderson, I. Building a Location Based Social Graph in Spark at InMobi https://spark-summit.org/2015/events/building-a-location-based-social-graph-in-spark-at-inmobi/

Another common form of data collection happens in the browser, which provides companies with insights into our interests, likes and behavior. Most, if not all, websites have third party trackers included in them. The visible trackers are the Facebook like button, Twitter bird and even the advertising on the page. These third party trackers are companies that are separate from the website, companies that offer the website specific services like advertising, analysis and social media share options. The purpose of data collection in the browser is for companies to collect data and build up a profile[4] of who we are: age, gender, where we live, what we read, and what we're interested in. This information can then be packaged and sold to others: advertisers, other companies, or governments.

Is the omnipresence of devices in our everyday life and the convenience of specific tools and services the sole reason that control is lost over personal data? No, data creation is more complicated then that. Data is created by us as a prerequisite for using a service – think of the data needed to register for Facebook or Gmail. Location and browser data is created when we interact with our devices. Other people tag us in social media. There are also more subtle ways[5] to create data about us. When we register for specific government, financial and social services, name, tax number, income, address and other data are required. When we move within and between cities, CCTV cameras and public transport systems are logging movements. Buying a plane ticket requires entering personal data and payment information into a website, which is shared at least with the airline and border police.

---

[4] Miljanovic, M. Profiling: glass data masks we wear unknowingly. Me and My Shadow https://myshadow.org/profiling-glass-data-masks-we-wear-unknowingly

[5] Sptiz, M. (2014). Was macht ihr mit meinen Daten? Woffmann und Camp

What is even more invisible is data about us that is inferred from other data. Data brokering companies create group profiles[6] on the basis of shared characteristics, based on social media networks, location data and/or browsing behavior. Our individual profiles can get tied to one or more group profiles, binding the group characteristics (data traces) to us. These group characteristics then become part of our individual profile, which can determine our credit rating, type of advertising and offers we receive. The problem is that we have no control over which group profiles we belong to, nor what inferred data traces are created and added to our individual profile.

Complicated? Let's take a fictional person, Renata, to understand inferred data. Renata lives in Rio de Janeiro, and spends most weekdays studying at the Universidad Federal. Her phone reports her location from there. On Friday and Saturday night, however, her phone reports back from the area Santa Teresa until around 4am, before returning to the location where it normally 'sleeps' (Renata's home on Rue Bento Lisboa). A data brokering company knows that many people who study at the Universidad Federal and go out in Santa Teresa also browse for vegetarian recipes and search for the latest rock concert. Based on Renata's movements, the company decides that she fits the profile of this group and labels her as a vegetarian rock-music fan.

---

[6] Miljanovic, M. Profiling: glass data masks we wear unknowingly. Me and My Shadow https://myshadow.org/profiling-glass-data-masks-we-wear-unknowingly

Why is all this data collected?

‘Data is the new oil.’ It does not matter whether this analogy is accurate. The truth is that there is a multi-billion-dollar data industry making money from our data. In the data industry companies range from data collectors, data cleaners, data sellers, all the way to attention sellers. Most of these companies have names we have probably never heard of, such as Acxiom, AdSquirt, Rubicon, CommScore and DoubleClick, whereas others are companies we might use on a daily basis, such as Google, Facebook, Linkedin and OkCupid. However, all these companies make money on data that is collected about us.

As a response to an in-depth investigation by the Federal Trade Commission (FTC) into the data broker industry[7], the oldest and one of the biggest data brokers in the US, Acxiom, gave people access to their personal data. Acxiom opened a website[8] that gave US citizens, after some bureaucratic processes, the ability to see, change and remove their data. In many instances US citizen who gained access to their Acxiom profile did not delete their data but changed it so that it would represent them better. This action moved them from being Acxiom’s product to becoming free labor for the company[9] by making Acxiom’s data sets more accurate and thus more valuable.

---

7 EFF. Data Broker Acxiom Launches Transparency Tool, But Consumers Still Lack Control https://www.eff.org/pt-br/deeplinks/2013/09/data-broker-acxiom-launches-transparency-tool-consumers-lack-control

8 https://aboutthedata.com/

9 Keen, A. (2015). Why the internet is not the answer. Atlantic Monthly

If our data is not saved by us but by the data industry, where is it? This is not very exciting: it is safe to assume that our data is stored in data centers all around the world. Our data is stored by multiple companies, and large commercial corporations like Google or Facebook do not store it in one location. These companies copy and store it in multiple locations. Individuals can only delete this data if the company gives them permission to do so.

What can we do to control our data?

The friction in increasing privacy and digital security as an individual is that companies and governments are becoming more and more sophisticated about collecting, analyzing and storing data, while we, the users, are made responsible for protecting our data with strategies and tools that only cover part of our digital traces. This does not mean that we should not do anything, but it does mean that we can only make it a little less bad and that all measures will have an expiration data.

The first steps to increase our privacy and take control of our data are actually surprisingly easy. Be aware of what is collected, where and who has access to it (other people, companies or governments), make choices about what data we want to keep private and which data we are comfortable sharing with others. Try the following steps:

1. Give as little data as possible. When we open a new email, social media or online shopping account or register for an event or a website or book a flight, several data pieces are requested. Limit the amount of data shared with companies by taking a critical look at the necessity of providing data for the use of a tool or service. Is this really necessary and or are there other ways? For instance, Twitter does not have a real name policy and enables people to create an account using a fake name with a random picture. However, the service still asks for an email address and mobile phone number. There is another way, though, because registering in the browser only requires an email account and not a phone number. Creating an anonymous email account is much easier than having an anonymous phone number.

2. Block tracking in the browser. There are some very effective bits of software that block trackers, encrypt website connections, or stop spying ads from running – all of which can make a big difference to our privacy. Apple recently allowed ad blocker in the App Store, enabling us to block third party trackers in the browser on our phones. Don't forget to clear the browser history and clear all cookies on a regular 'daily' basis.

3. Play around with default settings. Commercial Internet services have privacy settings which are often set to 'share as much as possible', but luckily this can usually be changed in our browser and on platforms like Facebook and Google. Remember that by changing the default setting, we are limiting the digital traces that will become public, but this does not mean the company that owns the platform will not collect it.

4. Have multiple identities. Play with separating your data profiles by creating different identities for communicating with work, family, network and friends. Try creating different identities for online shopping or use different browsers when accessing Amazon, Facebook, Twitter or Google.

5. Use alternative services. When we use commercial services for our email, chat apps, maps and file sharing, we share a lot of data with these companies. Using an alternative to these commercial services, will give us more control over who has access to this data. Find out which ‘alternative’ email services exist.[10]

6. Don’t forget the privacy and digital security basics. There’s no such thing as ‘perfect privacy’ or ‘perfect security’, but there *are* a few simple things we can do to keep our content, communications and web browsing more private and more secure. Keep our devices clean and healthy, use unique and strong passwords, install HTTPS everywhere, anonymize our Internet connection using the Tor Browser.

For more practical tips on managing your data, please visit us at myshadow.org and securityinabox.org

Fieke Jansen (NL) is a researcher and writer who aims for more transparency in the global data industry. Currently she works as the Project Lead for the Politics of Data program at the Tactical Technology Collective, which is an international organization dedicated to the use of information in activism.

---

[10] https://myshadow.org/increase-your-privacy#alternatives


Béton B.C.Ma
Crystal Computing gate 1
Cash-Métal
Deschieter

CENTER OF DOUBT

by Ivar Veermäe

Center of Doubt is a long-term artistic research project. The aim of the project is to explore and visualize the disappearance and reappearance of network technology, its infrastructure and representation. *Center of Doubt* is a collection of visual traces depicting the data industry of our times.

The appearance of the commercial 'cloud computing', or more precisely the data centers and their supporting infrastructure, is depicted as a turning point of a new era of centralized Internet: big corporations are in a competition to gain a fundamental status for their software and hardware, acting as a basic informational layer.

THE CLOUDS

I started my research by making video-based investigations about data centers, being interested in the material, local and environmental properties of the sites. I surveilled these technical buildings in Berlin, Tallinn and Frankfurt. The architecture of data centers has hidden or stealthy qualities, facilities are blended into cityspace. Being in the background is one of the main qualities of material infrastructure in general. This leads to a situation where what is actually visible is rendered invisible by being unobtrusive. In addition, there is an interesting gap between materiality and immateriality, which is intentionally ignored in representational rhetorics of IT companies. It is true that information is immaterial, but it is also true that material structures are needed to operate it.

Bruno Latour has a suggestion in his Actor-Network-Theory for thinking about things – make their role more important:

> Non-humans have to be actors and not simply the hapless bearers of symbolic projection.[1]

An actor, according to Latour, is meant as something/someone who/which influences the behaviour of other actors. Symbolic representation is offered often in finished and therefore closed form, which forestalls further discussion. In addition, when things are seen only as fulfilling the role assigned to them by their human creators, their role as mediator disappears.

The big things – data centers – in the cities remain hard to recognize, but more importantly, server farms are mostly hidden in remote places with suitable properties – like climate, taxes, but also security.

CRYSTAL COMPUTING (Google Inc., St. Ghislain)

Dear Sir,

We unfortunately do not organise or allow visits to our datacenters for data security reason.

This is the main reason why we setup a website where I am sure, you will find a lot of useful information on http://www.google.com/about/datacenters.

Thanks st-ghislain@google.com, 05.02.13

[1] Bruno Latour. Reassembling the Social: An Introduction to Actor-Network-Theory New York: Oxford University Press, 2005

I continued my research with Google's data center in Saint-Ghislain, Belgium. It is the largest Google data center in Europe and the second largest in the world. According to the official information from Google Inc., it housed 296,960 servers in 2013. After my request to visit the data center officially was rejected, I took a secret research trip to Belgium. The facility, located on the outskirts of of the small city St. Ghislain, is heavily protected – in addition to very strong non-human security – fences, CCTV cameras, motion detectors – there are also physical security guards circling the building every 30 minutes. The data center has water cooling, which produces colossal clouds of steam. This is reminiscent of old images of factories, but in fact it is a factory of 21st century.

The data center in Belgium has no visual traces of Google: the existing signs identify the place as Crystal Computing. Ironically, the name represents the secret policies of the corporation and also the establishment of subsidiaries as a method for tax avoidance. Interesting movements can be found in official founding documents of the Crystal Computing data center – representatives and capital have changed quite regularly over the course of few years.

THE FORMATION OF CLOUDS

As the Internet is currently becoming more and more a centralized corporate space, it is important to explore the immaterial thinking that has not changed so much during the course of 25 years. Previously dominant in the announcements of cyber-idealists, it is now used as a basic language in corporate advertising. Cyber-libertarians praised the ideology of immateriality, non-governmentality and libertarianism. '*A Declaration of the Independence of Cyberspace*', written by John Barry Barlow in Davos during the World Economic Forum (1996), is a perfect example of this kind of thinking:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. [2]

and:

> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter. There is no matter here. [3]

In this kind of conceptualization of cyberspace, which was supposed to be a home for pure mind in its immateriality, the mediatory role of technology is – probably consciously – forgotten. WIRED, the advocate and lobby agency of the Internet, concentrated mostly on *liberation*, which could be understood in a *libertarian*sense. In the beginning, the Internet had *libertarian 'wild-west'* characteristics, but soon it was capitalized. The main idea of cyberspace was communicated as a technology that connects humans, and therefore is radically different from exploitative industrial technology. Now it is clear that this kind of utopic cyberspace does not exist – there is no unified Internet, but mostly various corporate surfaces or spaces. It could be seen as a new wave of industrialism, or rather informationalism, which is supported by huge data-industrial buildings.

I am exploring this notion in *The Formation of Clouds* by concentrating on the formation of data centers, owned by world's leading digital companies – Microsoft, Apple, Facebook, Google and Amazon. The activities of these global network companies lead to highly centralized Internet access. The acknowledgement of the development of centralization on the infrastructural level is even more important, as user generated data is being stored and processed in data centers that are owned by private corporations.

---

[2] Peter Ludlow. *Crypto Anarchy, Cyberstates, and Pirate Utopias. Collection of essays.* Cambridge, MA: The MIT Press, 2001 → p.28

[3] ibid. → p.29

> Because the actual technological shape of the system is uncertain, whoever controls its first stages could decisively influence its future evolution. [4]

The most important aspect of *The Formation of Clouds* is that it reveals the competition between companies to gain the best possible position in running the basic underlying informational infrastructure of everyday life.

CORPORATE POWER AND DIY SERVITUDE

To understand the backgrounds of information technology, it is important to concentrate on the abstract notion of corporate power and its influences. According to Deleuze and Guattari, it is relevant to think about the concept of knowledge and its role:

> Knowledge, information, and specialized education are just as much parts of capital. 'Knowledge capital' as is the most elementary labor or the worker. [5]

Anti-Oedipus: Capitalism and Schizophrenia was first published in 1972, when major restructualization was just getting underway, and knowledge-based schemes began to evolve. Important changes that supported this system took place in the mid-70s and early 80s, as Manuel Castells writes:

---

[4] Christopher Steiner. *Automate This: How Algorithms Came to Rule Our World.* New York: Portfolio/Penguin, 2012

[5] Gilles Deleuze and Félix Guattari. *Anti-Oedipus. Capitalism and Schizophrenia.* London: Continuum, 1972

> In turn (1980s), the availability of new telecommunication networks and information systems prepared the ground for the global integration of financial markets and the segmented articulation of production and trade throughout the world. … Thus, to some extent, the availability of new technologies constituted as a system in the 1970s was a fundamental basis for the process of socioeconomic restructuring in the 1980s. [6]

It is important to notice that the changes to immaterial knowledge and information were directly dependent on the material developments of information technology. And conversely, material infrastructure was highly dependent on information. This system was the foundation for two principal fields:

> The new economy emerged in a given time, the 1990s, a given space, the United States, and around/from specific industries, mainly information technology and finance. [7]

There is a strong interrelation between the global financial system and information technology: could the former was able to develop through the latter, and the latter was dependent on the former. Information technology became a source of development and economic growth. These changes were realized in consumer culture, which was mainly oriented to youth. Origins of this idea – the adolescent as a perfect consumer – lay in US counterculture, as Fred Turner writes:

> Counterculture opened the doors of the youth movement to the complex delights of consumer culture. [8]

---

[6] Manuel Castells. *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. Oxford: Blackwell Publishers Ltd, 1996 → p.60

[7] ibid. → p.147

[8] Fred Turner. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: The University of Chicago Press, 2006 → p.32

The discovery or rather production of consumerism by various business enterprises created gigantic profits for them. According to Fred Turner, Steward Brand and the Whole Earth Network had an important role in these developments. In the late 60s the Whole Earth Network had published Whole Earth Catalogues. These were booklets containing information about various tools and thoughts, advertising a wide range of products – geodesic domes, tents, books about cybernetics and systems theory, but also microcomputers. The catalogue was a mixture of tool- and idea-set for back-to-the-land hippies with new information theory. By the end of the 1980s the Whole Earth Network had been transformed into Global Business Network. It was a business consulting firm using ideas that were a mixture of hippie ideology and entrepreneurship. GBN made connections between entrepreneurs, corporations, and government agencies. It supported two principal ideas, which had a huge influence later:

> corporation as site of revolutionary social change and interpersonal and information networks as tools and emblems of that change. [9]

Accompanied by:

> (Whole Earth) – Over time, the network's members and forums helped redefine microcomputer as 'personal' machine, computer communication networks as 'virtual communities', and cyberspace itself as the digital equivalent of the western landscape into which so many communards set forth in the late 1960s, the 'electronic frontier'. [10]

---

[9] ibid. → p.194
[10] ibid. → p.6

These two notions – the corporation as a site for social change and the 'personalization' of technology – influenced a clear move from politics to consumerism, from citizen to consumer, and from state to corporation. The main ideology of this movement is that one must liberate oneself. It is tricky, because one is never finished, therefore she/he must constantly develop themselves to achieve 'liberation'. As Deleuze clearly states in*'Postscript on Societies of Control'*:

> In the disciplinary societies one was always starting again (from the school to the barracks, from the barracks to the factory), while in the societies of control one is never finished with anything – the corporation, the educational system, the armed services being metastable states coexisting in one and the same modulation. [11]

One is never finished and must always modulate him/herself through the expression of her/his individuality. Bluntly said, nowadays consuming the products is transformed to being a product. Zygmunt Bauman and David Lyon have found a clever term for this – DIY servitude:

> 'Making oneself a sellable commodity' is a DIY job, individual duty. … The goods they (who) present as 'tools' for individual use in decision-making are in fact decisions made in advance. They were ready-made well before the individual was confronted with the duty (presented as an opportunity) to decide. [12]

The 'personal technology' one uses is never finished, it needs constant development. It is made for persons who are supposed to be making themselves using these products – yet forgetting their intermediary role. The hard- and software products are surfaces that only function when user feeds them with information. As Bauman and Lyon clarify:

---

[11] Gilles Deleuze. *Postscript on Societies of Control.* 1992

[12] Zygmunt Bauman and David Lyon. *Liquid Surveillance. A Conversation.* UK: Polity Press, 2013 → p.34

> All those technical gadgets are, we are told, 'user friendly' – though that favourite phrase of commercial copy means, under closer scrutiny, a product that is incomplete without the user's labour … not a voluntary, but a DIY servitude… [13]

The system is based on clever mimicry – free labor for corporations is masked as personal development – DIY, finding one's own liberation. One of the reasons why it works so well is found in the articulation: the corporate space, or rather the surface – the workfield – is named as a social network. On the one hand, naming commercial activities communal transformed the image of some corporations from greedy and evil to fun and likable. On the other, an ideal, utopian place, which was not accomplished by US counterculture, was transferred to Internet. In its beginning the Internet had a libertarian cyber-frontier character, but it changed under corporate domination. This is supported by corporate images – social, playful, pure, or innovative.

THE GIVEN

As a conclusion it is important to think about distractions, which could eventually stop further thinking. In big data based operations the person does not exist. The personal and private sphere is a distraction, which could divert attention to the actual person and the protection and improvement of this private sphere. Correlative mechanisms and algorithms deal with data in the form of data points, fixations, categories, and their relations. These are the given properties, which will be used to define various targets, or more exactly target groups. Data – a record of an actual event (textual, biological, chemical, geological) – could be justified through its existence. Bauman and Lyon write about the potential problem:

---

[13] ibid. → p.22

> Data double tends to be trusted more than the person, who prefers to tell their own tale. [14]

Data double is an abstraction that exists only in an anthropocentric view. But as a useful abstraction it has valuable qualities. Talking, explaining, or associating is uncertain, therefore it must justify its existence. This could be compared with the criminal process, where evidence is something that exists as a trace, whether biological, geological, chemical, digital. Through its existence it is justified, but still interpreted associatively by humans, who take uncertain aspects – motive, moods, etc. – into account. But a shift to the quantitative is happening in many domains, as Mayer-Schönberger and Cukier write:

> 'Big-data consciousness' – presumption that there is quantitative component to all that we do, and that data is indispensable for society to learn from. [15]

Since quantities are fixed categories, mostly based on events that have already happened, it is easy to justify them through their existence. Big data could appear to its users as given information, but more precisely it is the other way around – the user is the one who gives valuable information to companies and states. And since fixing is a stabilization, then it could influence the potentially changing user. With this situation the main problem is: how can one make bigger changes, when the predictions in form of suggestions are provided mostly by commercial companies, who are relying more on optimization and stability? Big data could eventually reach its etymological status – a (something that is) given (origin from Latin).

---

[14] Bauman and Lyon, *Liquid Surveillance. A Conversation* → p.8

[15] Viktor Mayer-Schonberger and Kenneth Cukier. *Big Data. A Revolution That Will Transform How We Live, Work and Think*. London: John Murray Publishers, 2013 → p.97

I explore the notion of quantification and big data in my videowork Patent Application Data. It is an attempt to go beyond the typical visual representation of data centers – blinking lights, cables, large sterile halls full of server racks. The patent drawings of data centers and their various processes provide a purified image that refers to the most important operations. Flowcharts, electrical schemes and machine drawings draw attention to the primary goals of data processing – to order and optimize the messy physical world.

> Move away from the age-old search for causality … instead we can discover patterns and correlations … The correlations may not tell us precisely why something is happening, but they alert us that it is happening. Big data is about what, not why. [16]

Ivar Veermäe's (EE/DE) work circles around questions of public space, networks and new technologies. As a result of long-term artistic research by means of photography, film and sound, his works are presented in versatile ways (such as video, on-site installations, interactive works and performances, also in public space). Ivar Veermäe aims to document and analyze the infrastructure underlying our contemporary culture of data and information. His projects show a processual, still evolving and therefore non-finite character that enables further discussions.

---

[16] ibid. → p.14


RTVA
Google
© 2012 Google
Report a problem
Image Date: July 2008

THE GOOGLE TRILOGY: OR HOW TO PLAY WITH GOOGLE STREET VIEW

by Emilio Vavarella

Borrowing the term "metamorphosis" from Elias Canetti's philosophy, my research revolves around what I define as "visual metamorphosis", through interdisciplinary art projects. According to Canetti, *metamorphosis* describes the essential goal of survival achieved through countless creative endeavors, and can be understood as that which enables humans to resist the power that dominates them. In his notes, Canetti explains how *metamorphosis* is the beginning of existence, what power is afraid of, what art should always create, and what has been expressed – since the beginning of time – in our dreams.[1] Indeed, a recurrent image in mythology is that of a human, who in order to escape from danger (some form of external power), transforms him/herself into an animal or a plant, and if that danger also changes its form to continue chasing its prey, the human will again transform him/herself, in a constant loop of metamorphoses. The history of art and literature are the richest repositories of such visions, and today the theme is so widespread (one must only think of contemporary posthumanism and transhumanism) that its prevalence can be compared only to its presence in the Greek and Latin traditions.

The concept of *metamorphosis* has adapted to the times, but its essence has remained the same. Stories of people shape-shifting into animals to overcome danger, such as an evil ruler or a bigger creature, were created at a time when large animals and despots embodied the highest idea of power. Today, stories of humans becoming machines, or networks, or integrating their bodies with technology to overcome superior threats confirm a similar attitude, updated

---

[1] Canetti, Elias. Massa e Potere. (English translation: Crowds and Power) Milan, Adelphi Edizioni, 2010.

for our contemporary society. These stories may take the form of scientific research, sci-fi film, literature or visual art (as in my case), and are always visual, since *metamorphosis* in its first stage is always a mental image. The concept of the body as data is the most natural conclusion: futuristic bodies will be copied and deleted, will disappear within a network, and resurface as new inhabitants of this Smart World yet to come. But as power struggles to control every step of this transformative process, and to channel its energy, the masters of metamorphosis resist any attempts of command and control (⌘ ❀) through countless subterfuges. A long time ago such practices were the prerogative of wizards, gods and shamans: for example there was Hermes in Greece, Eshu in West Africa, Krishna in India and Coyote in North America.[2] Their heroic and imaginative acts fill the pages of mythology. Now hackers and media activists play the same cathartic role: they perform ongoing and unpredictable mutations in the most controlled environments, and do good by cheating, bending rules and exploiting loopholes.

I can discuss my work *THE GOOGLE TRILOGY* (2012) as an example of my belief that technological power is the most significant today, and to exemplify the possibility of studying it (in the light of our current social and political situation) from an artistic perspective.[3]

The series of 100 digital photos called *Report a Problem* is the first part of this project. "Report a Problem" is the message that appears at the bottom of the Google Street View screen, which allows viewers to report a problem during the viewing of the place they are virtually visiting: missing censorship, wrong colors, random appearances. Only an image that is operative, that is put within a larger system of beliefs\functions can be considered "wrong". That's what happens in Google Street View, where images have the primary function of representing places in a realistic way. In 2011, while traveling in Google Street View, I started noticing images that could be simply defined as

---

[2] Hyde, Lewis, Trickster Makes This World: Mischief, Myth and Art. New York: Farrar, Straus and Giroux, 1998.

[3] See: `http://emiliovavarella.com/archive/google-trilogy/`

wrong. One image of a building, for example, presented something like a dimensional portal on top of it, another misplaced several elements, as though the landscape had been segmented into small pieces and then rearranged randomly. Fascinated by these virtual places I began saving their coordinates, so that I could find them again in the future. What I hadn't taken into consideration is that what I naturally considered beautiful data, was in fact for the majority of Google Street View' users just an annoying glitch. In fact, when I went back to those locations I found that most glitches had disappeared. Suddenly anonymous, boring views had rightfully taken the place of those surreal landscapes that had captured my interest: the magic was expiring. Therefore I decided to start photographing all of the wrong landscape I could find, creating some sort of collection of something that was destined to be erased as soon as someone reported the problem to Google. It was precarious data, time sensitive matter. That was around one year before the release of the project, and at that time I wasn't sure about the end result of my effort. Collecting images (I should say *certain images*) is also still part of my methodology, or organizing and transforming pre-existing materials, and at that time those weren't the only "wrong images" I collected. I had started, for example, a collection of screenshots of every single error notification visualized on my computer monitor. In that case I was interested in them being fake errors, or as Mark Nunes has explained in detail, "prepackaged errors"[4]. This term, as opposed to the "uncaptured error" is particularly important for my work with glitch aesthetic. A *prepackaged error* is a potential error, which is a fundamental part of the working mechanism of contemporary network society. It is also one of the instruments of technological power, which requires that error is always anticipated and caught (in some kind of feedback mechanism). The *prepackaged* serves and integrates technological power, acting as feedback and in other words explicating the norms and codes that define error in the technological realm. A common errors of this sort is in fact the *404*, which

---

[4] Nunes, Mark. Error, Glitch, Noise and Jam in New Media Cultures. New York: Bloomsbury, 2012.

appears on web browsers in the case of erroneous URL addresses, and that was one of the most common error in my screenshot collection. The "404" failure notices correspond to a potential error, something that the system has actually predicted before it occurred. Thus technological power transforms the virtual and potential opening of an error into a systematic closure: the *prepackaged* error message that we all receive conceals a successful operation from the perspective of the functioning of the system, and the potential error cannot but remain as such. What error would naturally imply, i.e. an opening to chance and the unexpected, is annulled. From the perspective of the system, the *404* error is always perfectly foreseen, and for this, its only remaining function is to act as feedback, useful for reinforcing the system's control. The landscapes I had found in Google Street View were very different: not only had they not been foreseen, but they had also escaped any form of "quality control" – perfectly representing the unexpectedness of a real technological error. With this in mind, my diary of error messages (which is still ongoing and now contains 3 years worth of prepackaged errors) functions as a personal encyclopedia of domestic errors, illustrating the pervasiveness, repetitiveness and banality of the control exercised on our networked spaces. Although the interest is still there, I haven't decided how to present this collection, yet. With the Google Street View Images, on the other hand, I knew that their aesthetic quality deserved something similar to a traditional exhibition: a photographic collection of the "rarest kind of technological errors": the uncaptured ones. The above description of prepackaged errors is in fact fundamental to contextualize both the rarity and the poetic openness represented by my *Report a Problem* photos. An *uncaptured error* is generally an error that refuses to collaborate with anything or anyone and disrupts efficiency in unexpected ways. The *uncaptured* is the sudden technological crash, the communication blackout, the hacker attack that disables the government website, the noise that interferes with data, an errant and aberrant signal. An *uncaptured* error always presents an excess that renders it not completely manageable, hence my desire to utilize and appropriate the

uncaptured does not imply taming it (in fact, as I said earlier, mine is a documentation of the presence of these errors, but similarly to the mere documentation of a wild species it doesn't exercise a strong control on the documented subject). Etymologically speaking, the errors in my *Report a Problem* series are the perfect example of real technological errors. As Nunes wrote:

> [An uncaptured error] calls attention to its etymological roots: a going astray, a wandering from intended destinations. In its failure to communicate, error signals a path of escape from the predictable confines of informatics control: an opening, a virtuality, a poiesis. Error gives expression to the out of bounds of systematic control. [5]

I continued to travel on Google Street View for a year photographing all the "uncaptured errors" I encountered before others could report the problems and prompt the company to adjust these wrong landscapes. Common landscapes are transformed in these images into something new. In the end, the work is presented as both a large scale photographic installation of 100 photos or a 5-minute long video slideshow of images.

The second part of the project, called *Michele's Story*, refers more directly to the cold impersonality of Google Street View's gaze. We all know that the service offers an immense public archive of panoptic images, the result of a systematic work which mechanically records aspects of life while avoiding human contact with the subjects photographed. At the time I was working on this series, each Google Street View car was equipped with a Dodeca 2360 camera with eleven lenses, capable of photographing 360 degrees. Afterwards the photos were assembled, creating a stereoscopic view, and an algorithm developed by Google automatically blurred the faces of people to protect the privacy of those accidentally portrayed. But,

---

[5] Mark Nunes. *Error, Glitch, Noise and Jam in New Media Cultures*. New York: Bloomsbury, 2012

I asked myself, even with blurred faces, what really happens to the images and stories collected in the process? My immediate answer was: they are both ignored and put on display. My second question was: is it possible to revert the de-humanizing approach that is at the basis of Google Street View? To find out I started working with Michele, a man who in 2007, as a result of an accident, became almost completely paralyzed and had memory damage. To contextualize my choice of working with him I have to say that the theme of memory has always had a major role in my work, as well as the fact of collaborating with other people, whether they are artists, scientists, or people I had met. At that time I had completed a project called *The Sicilian Family* (2012) that had required long interviews with my relatives in Sicily, through which I created a memory archive of my family. And more recently I've worked with the memories of Italian migrants in New York (*Memoryscapes*, 2015) and am trying to develop an artificial intelligence based on human memories for a drone (*Mnemodrone*, ongoing). Together with Michele, we used Google Street View as a repository of collective stories, a visual documentation of multiple memories, from which to pick the ones that resonated with his personal story. We slowly started to compose a sort of large scale puzzle, divided into 4 panels each presenting 25 details of images from Google Street View. Anyone who would look at the final photographic work could guess the story of a man going through a car accident and infirmity, interspersed with moments of deep sadness and solitude, poetical images and flashbacks from childhood conveying a contrasting sense of freedom and joy. The final collection of 100 photographs called *Michele's Story* is therefore composed of details taken from Google Street View and attempts to precariously reconstruct a single human journey by recovering snippets of stolen and dehumanized life.

The closing part of the trilogy, entitled *The Driver and the Cameras*, merges the topics of the previous parts. It expands the reflection on uncaptured errors from the first part with a focus on the "human factor" similar to the second part. The starting point of the eleven photos that compose *The Driver and the Cameras* (eleven refers to

the number of lenses used by the Google camera) was once again uncaptured errors. But these errors didn't affect the way a landscape or a urban environment was presented; it was specifically errors in the algorithm that automatically detected and blurred human faces. So, to create this third series I went looking for faces that had escaped this algorithm. The eleven resulting photos are portraits that immortalize the driver of the Google car. Eleven people, anonymous drivers, from Israel to the United States, portrayed in the act of cleaning or fixing the camera. Their proximity to the camera may have tricked Google's facial recognition software, or their presence may be the result of some other technical error. What's interesting for me is that the driver represents a sort of phantom power; he appears where he shouldn't be and his presence has escaped censure. His face is the symbol of an error yet at the same time shows a human side and, perhaps, the limits of technological power. We know from the writings of Norbert Wiener, father of cybernetics, that in relation to cybernetic systems, error speaks the "language of evil" [6]. So do these evil phantoms represent a menace for the system "Google Street View"? Is that one more reason to "fix" these images and quickly make the drivers disappear? If one important concern of the new aesthetic is how machines see us, would "ghosts" be a meaningful answer? Wiener in particular associated *uncaptured errors*, such as the driver portraits, with bad behaviors, intentional resistance, opposition to the system, or the possibility of someone causing disorder and failure. Still, the subjects of these photos are workers, invisible but indispensable humans behind the cascades of data that Google organizes. In Wiener's vision, the *uncaptured* error is the demon that wants to see the world burn, but also the gap that opens up a dangerous breach in the faith in the system. I believe these errors are very far from demoniac presences, but they strongly undermine our faith in the perfection of technological systems: on one side they remind us that there are still humans sweating behind virtual realities, and on the other side they remind us that technological

---

[6] Wiener, Norbert. The Human Use of Human Beings: Cybernetics and Society. New York: Da Capo, 1998.

systems are fallible, just like people. This gap in the control of the system, which corresponds to the culmination of anxiety in Wiener's cybernetic systems, brings our attention to the gaps or interstices of power: the weak points in the system. It is precisely these interstices that interest me and function as a catalyst in my art projects. These ambiguous spaces, according to Wiener, occupied by a "malevolent potential", become my field of action. They represent the connection point between my interest in errors and my interest in metamorphosis. When we consider metamorphosis as a creative transformation and we accept the unpredictable creativity of errors, we reach the certainty that error is a fundamental element in metamorphic processes – an idea that would make many biologists nod in approval. To conclude, experimenting with technological errors towards new visual *metamorphoses* offers the unique opportunity to understand the hidden structures of the technological power that surrounds us, while also proposing ironic, poetic, and unexpected ways to resist its most menacing effects: command and control.

Emilio Vavarella (IT/USA) was born in Monfalcone (Italy) in 1989. He graduated summa cum laude from both the University of Bologna with a B.A. in Visual, Cultural, and Media Studies, and from Iuav University of Venice with an M.A. in Visual Arts and study abroad fellowships at Bezalel Academy of Tel Aviv and Bilgi University of Istanbul. Emilio's work has been recently shown at: EYEBEAM, ISEA, SIGGRAPH, *GLITCH Festival,* Media Art Biennale, European Media Art Festival and Japan Media Arts Festival. His work has been published in: ARTFORUM, Flash Art, Leonardo and WIRED. He currently lives and works in New York.


PLACE
GRACE
PLACE
GRACE

SURVEILLANCE, MCLUHAN, AND THE SOCIAL PROSTHESIS: EXAMINING THE CONSTRUCTION AND PRESENTATION OF IDENTITY

by Leo Selvaggio

In 2014, I launched *URME Surveillance*, an artistic intervention that protects the public from facial recognition surveillance systems by allowing them to wear a photo-realistic 3D printed prosthetic of my face. When a user dons the prosthetic, cameras equipped with facial recognition are likely to identify the wearer as myself, thus attributing all of their actions in surveilled public space to the identity known as "Leo Selvaggio." In this way, wearers of the prosthetic safeguard their identities by convincingly performing my own in surveilled areas.

In addition to protecting the wearer, *URME Surveillance* also subverts and confounds large systems of surveillance through the creation of disinformation, primarily through asserting the presence of my identity to surveillance systems in various areas of public space simultaneously. For example, if multiple users were to wear this prosthetic and become "Leos" in different areas of the same city at the same time, facial recognition systems would have conflicting locative information: the identity "Leo Selvaggio" would be inhabiting Main St, Carmen Blvd, Michigan Ave, and so on. Additionally, as the body of each individual wearer is different, there may also be inconsistent or contradictory data gathered about my height, weight, and gender. When done on a large enough scale, these conflicting data sets call into question facial recognition systems' ability to accurately determine the true identity of any face captured in camera-based documentation. This subversion becomes all the more relevant as surveillance practices traditionally conducted by human beings are increasingly being turned over to automated systems under the false supposition that such systems are accurate and free of bias, which we will see is not the case.

URME Surveillance successfully corrupts digital surveillance networks through an analysis and exploitation of the way those systems function. Facial recognition technology, as it is applied for practical use, operates on the assumption that faces are unique and inherently tied to individual persons. This assumption of stability when collecting data on faces (and their respective identities) is what produces our confidence in statistics and lends that data enough credibility to be considered incriminating judiciary evidence. Rather than attempting to subvert this system through digital means, *URME Surveillance* takes an analogue approach, turning the system's assumption of stability into a weakness by producing conflicting data sets in facial recognition databases.

Compared to several other digital interventions, such as Julian Oliver's "No Network" piece, *URME Surveillance* is a relatively low-tech project. Though the *URME Surveillance Identity Prosthetic* is not a digital interface, its effect and execution are digital to some degree. Within the logic of *URME Surveillance*, one is either performing "Leo Selvaggio" or they are not. Functionally, *URME Surveillance* is similar to a computer virus. As each wearer becomes a part of the *URME* worm, "Leos" multiply and replicate, confounding data sets about the "Leo Selvaggio" identity. In this way, *URME Surveillance* engages and empowers the public as active collaborators and components of a larger network of human interaction.

This idea of writing and rewriting my identity like code within a social network has been a thematic component of my work over the past five years. Recent digital technologies have changed the models of both production and distribution of contemporary popular media. With the advent of smart phones, affordable software like iMovie, and social networks like Facebook, LinkedIn, and Vimeo, the amount of user-generated media is at an unprecedented high. The larger aim of my work, even outside the scope of surveillance, is to explore how this shift in technologies relates to the construction and presentation of identity in the social arena, an increasingly prevalent practice that sits at the core of our culture.

Perhaps Marshal McLuhan said it best when he coined his prophetic term the "global village" in his 1962 book *The Gutenberg Galaxy*. McLuhan states:

> The next medium, whatever it is – it may be the extension of consciousness – will include television as its content, not as its environment, and will transform television into an art form. A computer as a research and communication instrument could enhance retrieval, obsolesce mass library organization, retrieve the individual's encyclopedic function and flip it into a private line of speedily tailored data of a saleable kind.[1]

Especially eerie is McLuhan's prediction of this "private line of speedily tailored data of a saleable kind." Recent news is flooded with reports of companies such as Google, Facebook, and Microsoft selling user information to marketing firms. For example, in section three (titled "privacy") of the terms of use for Xbox Live, a Microsoft affiliate, we find:

> In particular, we may access or disclose information about you, including the content of your communications.... Personal information collected by Microsoft may be stored and processed in the United States or any other country or region in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities. You consent to any such transfer of information outside of your country or region.[2]

What Microsoft makes clear is that personal information – or aspects of identity – can be digitized, collected, and distributed via McLuhan's theory of the global village network.

In fact, a recent 2013 study from Cambridge University claims that key aspects of an individual's personality can be determined through an analysis of the "like" button:

---

1 Marshall McLuhan. *The Gutenberg Galaxy; the Making of Typographic Man*. Toronto: University of Toronto, 1962

2 Xbox.com. *Xbox LIVE Terms of Use*. 2011

> We show that easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. [3]

While it should be noted that one of the researchers is associated with Microsoft, and therefore stands to profit considerably from this study as a shareholder of Facebook, what is at the center of the study is the notion that the choices we make on social media sites are predictive indicators of how we are perceived by both corporate America and by everyone in our global village network. Our identities are no longer products of our own doing. They are no longer constructed by the choices that we made growing up, reflected upon and affirmed by the infinitesimally small percentage of people in the world with whom we spent the majority of our time. Identity is now created through the perception of millions by what we like or don't like on Facebook. How can one possibly navigate this change? How can we talk about the self when its creation is now proliferated via a faceless conglomerate workforce of hashtags, retweets, and reposts?

The answer may come from McLuhan when he states in his 1972 book *Take Today: The Executive as Dropout*:

> Paradoxically electronic man has no choice but to understand processes, if he is to be free… The only method for perceiving process and patterns is by inventory of effects obtained by the comparison and contrast of developing situations. [4]

---

[3] Michal Kosinski, David Stillwell, and Thore Graepel. "Private traits and attributes are predictable from digital records of human behavior". In: *Proceedings of the National Academy of Sciences of the United States of America (PNAS)* (2013)

[4] Marshall McLuhan and Barrington Nevitt. *Take Today; the Executive as Dropout*. New York: Harcourt Brace Jovanovich, 1972

Here, I would propose that McLuhan is advocating a subversion of digital technology's reduction of our identities into quantifiable and categorical information by using the very same infrastructure for our own purposes. If the Internet is going to send our "data" to and fro, then let it do what it does best, but we must control the content of that data. We, the users of the web, the public, must be the generators of the messages sent through our networks. We must write the software of our identities rather than settle for being its referential hardware.

How we go about doing this comes from the second portion of the McLuhan quote above, in which he describes the method for "perceiving process" as an understanding of the cause and effect of actions in "developing situations." When applied to the presentation of our identities in our digitally mediated world, we are looking not at a passive understanding of networks like Facebook, but rather the development of a viable skill.

To understand this, let's look at common social practices on Facebook. Facebook gives to our identities what texting and email gave to our verbal communication: a chance to edit our messages. Rather than reacting in the way a personal physical interaction requires, email allows us to parse through our thoughts and craft carefully constructed responses. In a very similar way, Facebook gives the time required to present our best self. Whether it be rewriting posts for maximum humor, choosing which photos of ourselves to upload and which to discard, detagging ourselves from others' posts and photos, or most recently, using the "groups" function to dictate our content's audience, Facebook is an intermediary between our full selves and the expression of ourselves that we put out into the world. In other words, it is a curatorial practice. It is this skillful social editing that facilitates the creation of networks of influence: "friends," in Facebook terms.

Klout.com provides us a useful example of this influence through their unique "scoring" system:

> Klout's vision is to enable everyone to discover and be recognized for how they influence the world. With the rise of social media, the ability to impact others has been democratized. Klout measures your influence based on your ability to drive action on social networks. The Klout Score is a single number that represents the aggregation of multiple pieces of data about your social media activity. [5]

A shocking example comes from the comparison of the Dali Lama and Perez Hilton's Klout scores. The Dali Lama, beloved spiritual leader recognized around the world for his influence, has a Klout score of 86 (out of 100), with which he influences 758,000 followers via social media [6]. His score is pretty good – twice my own. However, self-made blogger Perez Hilton has a score of 90. The fact that Perez has a higher Klout score is just spectacle, but it does highlight the different spheres of influence that lend each figure his authority. While the Dali Lama's influence is attached to his station as a spiritual leader, Hilton's influence comes entirely from his skill at controlling social media. Hilton has a standard education – a BFA in theater. He did not come from money, and he represents a marginalized community as an openly gay, albeit white, man. His success comes solely from his ability to network within the blogosphere and to influence not only others' perception of himself, but others' perception of others as well.

The presentation of identity is not only an invaluable skill, but an active task. It requires maintenance and constant production and distribution. As we have examined within this new context of a technologically and socially mediated identity, if one does not control the content of the message, others will. The *URME Surveillance Identity Prosthetic* exemplifies this by transforming my identity into tangible material for others to present. Who I am, in part, becomes based on the surveillance data

---

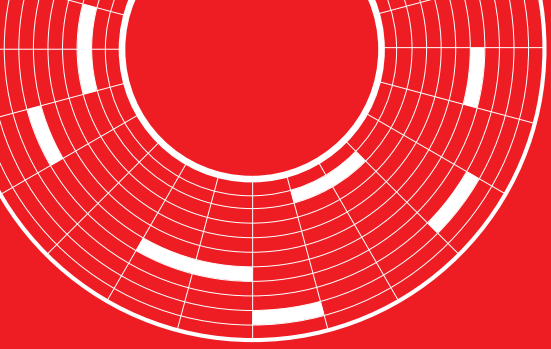
5 Klout.com. *Klout Score*

6 Mythreyi Krishnan. *"Influence Metrics for B2C Brands." The JamiQ Blog*. 2011

collected about me which is produced by others, much in the same way "likes" on Facebook are collected to produce marketing profiles. In doing so, the work exposes the underlying systems threatening the authorship of individual identity, by allowing others to challenge the authorship of my own.

In doing so, what *URME Surveillance* highlights, as do several of my other works, is the malleability and vulnerability of identity within a technological context, and it empowers its audience to consider how they construct, present, and author their own socially mediated identity. Lastly, it is important to note the opportunity to produce and present identity as a means of harnessing collective power. Identifying that opportunity as a cultural practice that can be formulated into a skill is perhaps the most important development in understanding how to resist and defend our individual authorship. To the conglomerate effect of this production and distribution of content as it refers to the presentation of our identities via digital networks for the purpose of, as McLuhan states, "being free", I offer the term social prosthesis: the total manifestation of one's creation, navigation, and maintenance of relationships that comprise the web of that individual's network of influence.

Leonardo Selvaggio (USA) is a Chicago based interdisciplinary artist whose work examines the intersection of identity and technology. He has shown work internationally in France and Canada; domestically in New York, Chicago, Florida, and New Mexico. He has been awarded an Albert P. Weisman grant for his work, *URME Surveillance* and a DCASE IAP Professional Grant to present supporting research. That artistic intervention invites users to wear a photo-realistic prosthetic of his face as protection from pervasive facial recognition surveillance systems. URME has been selected for the Art Souterrain festival in Montreal, the ISEA conference in Vancouver, and the Saint-Etienne Design Biennial in France. In 2015, *URME Surveillance* was also adapted for television in an episode of CSI: Cyber titled "Selfie 2.0".



DELETING DATA

What remains?
The way we save ourselves

by Marloes de Valk

> When it was announced that the Library contained all books, the first reaction was unbounded joy. All men felt themselves the possessors of an intact and secret treasure. [1]

Never before in history have we been able to record ourselves in such great detail. A couple of photo albums and a box with old letters have turned into a continuous stream of descriptions of our lives through an ever expanding amount of photos and messages on social media as well as on our mobile devices. On those devices there is a plethora of apps available that try to generate meaning out of personal data. “Self knowledge through numbers” [2], the Quantified Self. What started in the nineties in the livecast scene with Steve Mann’s Wearable Wireless Webcam and the Jennicam, a 24/7 recording and broadcasting of the life of Jennifer Ringley by Jennifer Ringley, has now become a lifestyle for the masses. Where does this need to record and document ourselves come from? It seems as if we’re suffering from an existential fear, that if we don’t save as much of ourselves as possible, all this precious information revealing truths about us, giving meaning to our existence, will be lost. Can we, by becoming our own Big Brother, reach a deeper understanding of ourselves, become better people, as suggested by the Quantified Self movement?

---

1 Jorge Luis Borges. *Fictions*. London: Penguin Books, 2000 → p.69

2 The Quantified Self is an international collaboration of users and makers of self-tracking tools.

Our hunger for information started with the shift in meaning of the word information itself[3]. Information used to mean nothing more than a short statement of fact, such as a number, date or place. Nothing so special you would name an age or type of economy after. In the 1950s this changed with the advent of cybernetics, the study of feedback in self-regulating closed systems, where information was seen as the means to control a system, any system, be it mechanical, physical, biological, cognitive or social. Wiener, a mathematician and father of this then new field of research, stated "To live effectively, is to live with adequate information. Thus, communication and control belong to the essence of man's inner life, even as they belong to his life in society"[4], and only ten years later, in 1958, Artificial Intelligence researchers Simon and Newell wrote "the programmed computer and human problem solver are both species belonging to the genus 'Information Processing System'"[5] skyrocketing the value of both information and computers to a mythical height, implying both are able to bring us closer to the secret of human consciousness. In the seventies it was granted an even more powerful status, that of commodity. AT&T said it best: "Like it or not, information has finally surpassed material goods as our basic resource"[6]. Bon apetit.

---

[3] Theodore Roszak, "Information, please", in The Cult of Information: The Folklore of Computers and the True Art of Thinking, (New York: Pantheon Books, 1986), pp. 3-20.

[4] Norbert Wiener. *The Human Use of Human Beings: Cybernetics and Society.* Boston: Houghto Mifflin, 1950 → p.17

[5] Joseph Weizenbaum. *Computer Power and Human Reason.* San Francisco: W.H. Freeman, 1976 → p.169

[6] AT&T advertisement in Kiplinger's Personal Finance, October 1985, p.33.

So here we are, more than half a century later, generating a deluge of digital information, the new gold. In fear of a digital dark age we cling to it while leaking it out of every port of our computer. How do we protect the object of our passion from being lost to the mists of time? We make back-ups and pray the Cloud will protect us, for we believe to risk more than losing our family pictures, we believe we could lose the chance to better understand ourselves, our society, even life itself.

Is this fear grounded? Besides the question of whether there is anything of value to be found, is it hard to save digital data truly long term? We face quite a few obstacles. The main problem is that data, even though it has a very immaterial ring to it, needs a physical carrier, and this carrier has a limited lifespan. Even though it feels as if we've made incredible technological advances in the past seventy years, we still struggle to find reliable carriers. Another obstacle is obsolescence, both when it comes to hard- and software. To maximize profits the industry has set a rapid pace for updates. Both the machines that host, the software that is used to create and the formats to save the data are replaced. Which brings us to the economic factor . . . storing data is not cheap. It involves more than updating and maintaining hardware, you also have to keep the data retrievable, and when it comes to large data sets this requires two pricey things: manpower and considerable amounts of electricity.

How do you save data that is part of an ever changing and dynamic environment such as the Internet? It supposedly never forgets, but take for example the data on a social media platform: it is highly context dependent and its survival relies solely on the lifespan of the company owning the data and on its policies regarding the archiving and publication of its content. This hints towards the

legal problems surrounding data storage. Who owns it and therefore has control over it? Most social media platforms, for example, have no legal obligation towards their users, and have complete ownership of the data users provide them with. And if it didn't prove to be enough of a challenge to overcome all these obstacles, there is the issue of data proliferation: the shear amount of data we're trying to save is absolutely phenomenal and ever increasing.

We're obsessed. Our data bodies morbidly obese. Metaphors like the cloud promise infinite liposuction, delegating the storage of our excesses to what seems like outer space. It feels as if there is no need to be selective, storage space seems limitless to individuals, we are offered free storage just about everywhere, at no cost. And in the end, most of us trust there will be a technological solution offered to solve the aforementioned issues. Perhaps our indifference is in part influenced by the way we describe technology. Putting your data in the Cloud sounds like a perfect solution, it has beautiful connotations: safe, clean, lightweight, natural. The Cloud metaphor hides the uglier and riskier reality of data centers filled with energy-consuming, heat-producing, maintenance-hungry servers. Other metaphors, such as Data mining and Data streams, compare data to naturally occurring physical resources, seemingly inexhaustible and ready for exploitation in the name of economic growth and private gain. They mask the human aspect of it, the fact that most of it is personal, something we would be more hesitant to have exploited.[7] Other metaphors, such as open data and software transparency have strong connotations of trust. If everything is open and transparent, everyone will behave

---

[7] Tim Hwang and Karen Levy, "'The Cloud' and Other Dangerous Metaphors, Contemporary ideas about data and privacy are tied up inextricably with language choices", The Atlantic, January 20, 2015, http://www.theatlantic.com/technology/archive/2015/01/thecloudandotherdangerousmetaphors/384518.

honestly. But the sheer amount of online scams show transparency is no guarantee, hiding in plain sight is easy in an environment where real and fake are indistinguishable. The Cloud, data mining, transparency and openness, these metaphors hide the darker effects of our obsession: the privacy we've lost, but also the fact that information is not immaterial, the waste we produce, the electricity that is consumed all have a real impact.

Our connected and information-hungry lifestyles feel as clean as the design of our latest gadget, but that is only because we export many of the dirtier sides of it to the less privileged parts of the world, where labor is cheap and there is limited regulatory oversight into health, safety and environmental impact. Near Baotou in China, for instance, the effects are clearly visible and took the shape of an artificial toxic lake of black sludge, the result of mining to create our tech gadgets.[8] China is also home to one of the largest dumps of e-waste in the world, which not coincidentally is also one of the most polluted places on earth: Guiyu. Despite strict regulations, loopholes have been found and illegal dumping of e-waste in countries such as Ghana and China is still happening under the guise of aid or second hand goods. In 2010 as much as 75% of the 8.7 million tons of e-waste generated in the EU could not be accounted for, despite regulations. In the US the figure is said to have been about 80%.[9] Only because we're running out of certain metals and mining them becomes increasingly costly, have we begun to recycle old hardware in the developed world. Initiatives like "Closing The Loop" are buying and recycling old mobile phones from the

---

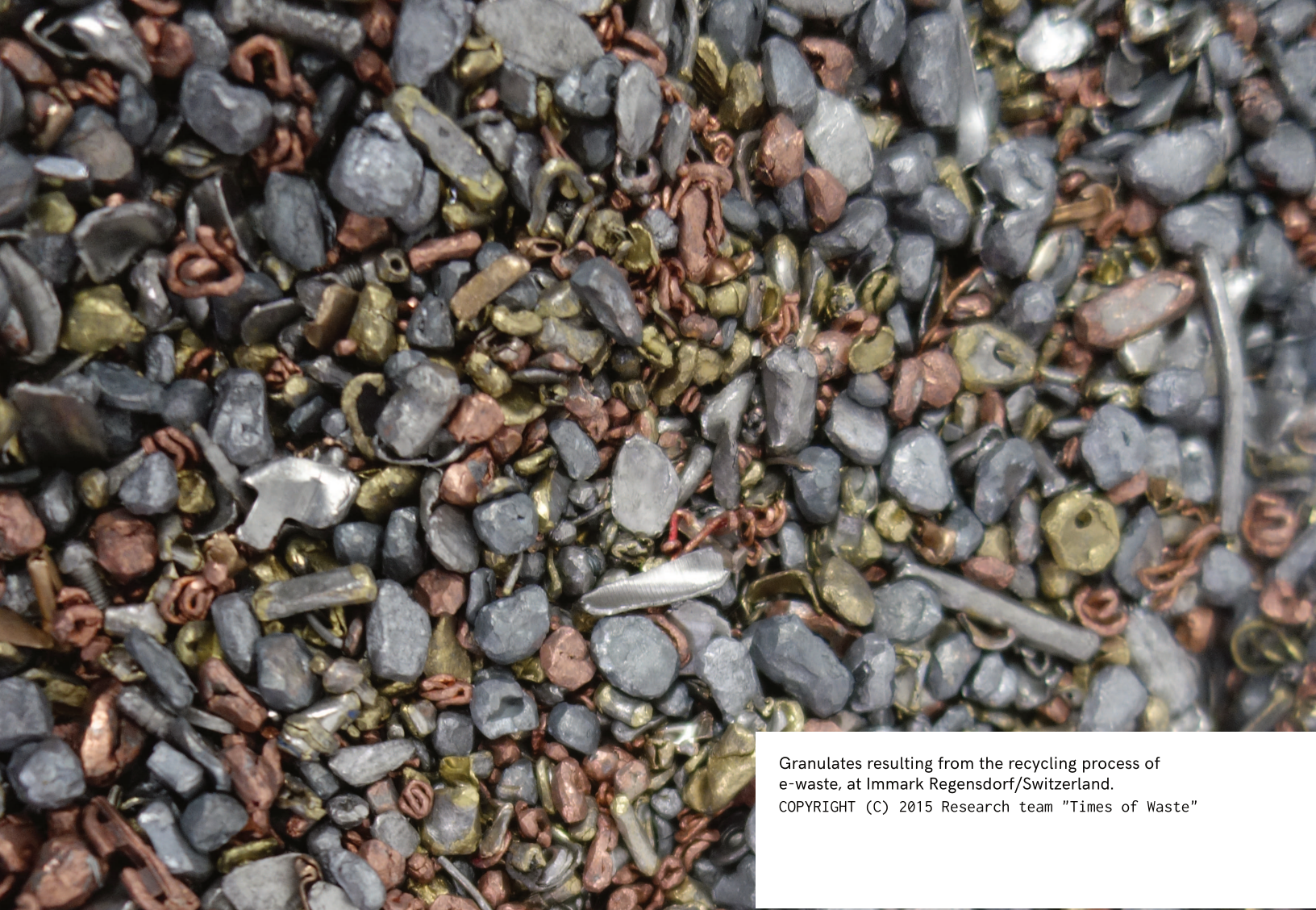
[8] Tim Maughan, "The dystopian lake filled by the world's tech lust", BBC Future, April 2, 2015, http://www.bbc.com/future/story/20150402theworstplaceonearth.

[9] Orish Ebere Orisakwe and Chiara Frazzoli. "Electronic revolution and electronic wasteland: The West/waste Africa experience". In: *Journal of Natural Environmental Sciences* (2010) → p.45

countries we previously used as a dump. After decades of poisoning, we are back at mining for gold, perhaps diminishing pollution, but keeping the economic inequality intact. From poor working conditions in electronics manufacturing plants and e-waste pollution to energy-hungry server farms and our loss of privacy, the disastrous effects of our lifestyles can be felt on so many levels it hurts to think about it, and that is probably why we don't.

We consume information at high speed but forget even faster, repeating the same behavior as if the news has been overwritten with Internet memes and enhanced photos of our latest attempt at cooking. The real treasures in this tsunami of data are the ones that give us a chance to see past tomorrow, to see the long term consequences of our choices, the big picture. But all that most of us can still distinguish is noise. Future historians can go in search for the big ideas of our time inside what is left of the machines we've build to keep our treasure. They might analyze what is left of the data we've produced. One idea of our time will surely remain, our information fetishism.

Marloes de Valk (NL) is a software artist and writer in the post-despair stage of coping with the threat of global warming and being spied on by the devices surrounding her. Surprised by the obsessive dedication with which we, even post-Snowden, share intimate details about ourselves to an often not too clearly defined group of others, astounded by the deafening noise we generate while socializing with the technology around us, she is looking to better understand why.



Granulates resulting from the recycling process of e-waste, at Immark Regensdorf/Switzerland.

Silver raw material with high purity of 99.98%,
storaged as asset by Schweizer Metallhandels AG.

TIMES OF WASTE

by Research Team "Times of Waste"

> The ecological thought is also difficult because it brings to light aspects of our existence that have remained unconscious for a long time; we don't like to recall them. It isn't *like* thinking about where your toilet waste goes. It *is* thinking about where your toilet waste goes. [1]

The research project "Times of Waste" is the follow-up of our research and exhibition project *RhyCycling,* which examined the border region of Switzerland-Germany-France along the river Rhine. As its title indicates, playing with the words *Rhy* (for Rhine in Basel's dialect) and *recycling,* the river and its surroundings in Basel were conceived as a network. [2] We saw a mesh of different human and non-human actors (like fish and ships), activities, and circulations of goods. And we saw circulations of garbage and scrap, tons of contaminated soil and toxic stones. This ugly grey mud and beautiful colored sediments were the geological remainders of Basel's industry dating back to the end of the 19th century. They have been removed and purified to build the next generation of chemical industry, the Novartis Campus. To provide the citizens with a promenade along the Rhine, traversing the border between Switzerland and France, residual lindane is still being cleaned out of French soil.

---

1 Timothy Morton. *The Ecological Thought.* Cambridge, MA: Harvard University Press, 2010

2 See e.g. Bruno Latour: Das Parlament der Dinge: Für eine politische Ökologie, Frankfurt am Main, 2009.

THINKING IN LONG CHAINS

On the basis of current network, subject, and materiality theories, we depict waste as a dynamic, transformable and living matter affecting and involving many actors and entities.[3] Using scientific and artistic practices the research project examines the purification, treatment and reuse or disposal of objects and materials as well as the actors and fields of activity involved. On the transport and recycling routes extending from Basel's local context into global connections, objects undergo not only material transformation, but also economic, social, aesthetic or rhetorical reassessments. What is considered waste or respectively a "new" resource, when or at which stage of materiality, is a question of perspective and interest. Our project partner, the historian Bernd-Stefan Grewe, for instance, defines waste or garbage as "objects which are in the wrong place"[4]. This is an assumption we would like to agree with, with the exception of nuclear waste for which there can be no right place.

We asked questions like: What are the transformation processes and value changes of (waste) objects or materials? What material changes do they undergo from creation to reprocessing or disposal and removal? How are specific actors involved in these processes? And finally: How can a topic like this be presented for public reception using transmedial techniques?

In order to be able to go more into detail, we chose three exemplary objects/materials that we wanted to trace, thus creating an object biography in various media. We chose the smartphone, urban mining (recycled material from buildings, streets etc.) and nano-silver. The smartphone has been chosen for the following reasons:

---

3 See Bruno Latour 2009; Donna Haraway: A Cyborg Manifesto, Routledge 1991; Gilles Deleuze/Félix Guattari: A Thousand Plateaus, Minneapolis 2001; Jane Bennett: Vibrant Matter. A Political Ecology of Things, Durham 2010; Timothy Morton 2010; Jennifer Gabrys: Digital Rubbish: a natural history of electronics, University of Michigan Press, 2011; Jussi Parikka: A Geology of Media, Minneapolis 2015.

4 In this context, see also Bernd-Stefan Grewe: "Raum und Macht – Eine Stoffgeschichte des Goldes im frühen 20. Jahrhundert", in: Jahrbuch für Wirtschaftsgeschichte 57/1 (in print)

1. It is a consumer fetish, a beautiful object with a clean and smooth surface. But if you go "behind the smart world", you realize that there is "dust and exhaustion" (Jussi Parikka).
2. It is designed to be dumped. With its miniaturized high-performance electronics that make it difficult to repair, with a primary user cycle of 18 months, and the sheer masses and ubiquity of its presence, we could say it has already been a piece of garbage from the beginning.
3. Its ubiquity, smallness, and global presence make it the prototype of our new state of machinic being, always connected, always hyped up.

We were looking for gaps in the cycles, trying to meticulously follow the paths and circulations of its components. Now, after having worked for almost a year on e-waste generally and the smartphone biography specifically, we have to say that we did not expect our enterprise to become divided into such small sections. There is never only one path; at every section and/or component, there are manifold possibilities of its disposal or further life-cycle. Especially with the smartphone, things seem to be much more complicated, because it does not always follow the "usual routes" of e-waste. Even the simplest way, the legal transformations in the scrap and recycling factories, turns out to be a long and complicated sequence of paths inland and abroad. Despite all our efforts, we haven't been able to fully follow the trail until the very ends of the different slags and newly won metals. At first it seemed that this route would be so easy, because Switzerland really tries to face the problem caused by e-waste. When an electronic device is purchased, the consumer pays an anticipated recycling charge of around 5% of the selling price. In return, she can bring back her gadget at every point-of-sale, and the point-of-sale gets money for bringing them to the next step in the recycling process.

In contrast to other electronic waste, smartphones contain such a high amount of reusable metals that they are usually not mixed and shredded with other devices, but – after removing the rechargeable battery – they are brought directly to the smelter. But what sounds simple in theory is more complicated in reality: Further research showed that, in fact, in

Switzerland most smartphones don't go to the regular recycling system. Many of them are presumed to be still lying in the drawers of their owners, although no longer in use – it's a personal item with all your data, after all. And then there is a high tendency to reuse and export smartphones, since they are usually given up by their primary users when still functional. Where exactly these used smartphones end up going and how they flow into the local recycling economies is something we have to explore further.

Second, we found out that the smartphone does not emit most of its waste after, but before its consumption. It is the mining industry, the usually opencast pit mining of the smartphone's almost 60 metals and rare earth elements, which produces huge amounts of toxic and – in the case of neodymium – radioactive waste, in addition to the fact that it depletes human beings. Although the number of smartphone users was 1.59 billion in 2014, it is presumed that the number of users will grow to more than 2 billion in 2016.[5] Since smartphones are only used for about 18 months by the primary user, this will keep both sales rates and electronic waste from smartphones high – even though the tonnage of garbage caused by smartphones is comparatively low, due to their low weight (140 g / piece on the average).

This result contradicted our first assumptions and led us, contrary to our initial plans, to examine the conditions of production, i.e. the conditions of mining and trading metals and rare earth elements.

Although rare earth elements are not generally rare (but hard to mine and spread all over the world), this is actually the case with neodymium, which is used to build the smartphone's magnet, for instance. Research institutions have recently been putting great effort into extracting neodymium from used magnets or finding substitutes, because western nations do not want to depend too much on China, which owns the world's biggest

---

5 www.statista.com

pit. Despite the generally positive results concerning extraction possibilities and their costs, there are still open questions regarding the technical feasibility of the whole recovery chain.[6] Thinking about future political consequences, one of our interviewees, Heinz Böni, head of the Technology and Society Lab Empa, mentioned that the "extended producer policy", a worldwide standard, would gain another dimension with an obligation to recover rare earth metals. But political processes are slower than research findings. Also some experts think that providing extra money for better collecting systems, for example, would be environmentally more efficient than recovering neodymium from the comparatively low percentage of recycled smartphones at the moment. The far-reaching consequences that may be caused by restrictions became evident in the US law Dodd-Frank: It caused a quasi boycott by multinational companies, for instance, of minerals of Central African origin supposed to be from mines in local conflict areas. Initiatives like the iTSCi program (ITRI Tin Supply Chain Initiative), a joint industry project designed to address conflict mineral concerns in the Democratic Republic of Congo (DRC), Rwanda and other countries of the Great Lakes Region, attempt a counter-strategy to combat the resultant unemployment. As our interviewee Mickael Daudin, reporting officer of the iTSCi program, mentioned, their program establishes traceability and due diligence in the upstream mineral chain – from the miner to the smelter – by working with local governments and their field agents. By allowing companies to source metals responsibly, total disengagement from the Great Lakes Region can be avoided.[7]

The "Konzernverantwortungs-Initiative"[8] – "global business, global responsibility" – launched by Swiss NGOs in spring 2015 seeks to bring transparency to the trading chains of multinational companies based in Switzerland, which are currently only voluntarily made transparent and traceable. Human rights, social and ecological standards for mining raw

---

[6] See e.g. the E-Recmet study; Heinz Böni et al. Indium und Neodym: Ist ein Recycling sinnvoll? Fachbericht 2015, p. 19-20.

[7] https://vimeo.com/44562369

[8] https://www.evb.ch/kampagnen-aktionen/konzernverantwortungs-initiative/

materials and transparency throughout the whole trading chain should become a standard and, in case of accidents, the corporations would have to take responsibility. These actions seem to be a more integral way to raise consciousness for raw materials and their global entanglements than Dodd-Frank is.

METALS NEVER DIE, THEY GO ON AND ON AND ON . . .

In short, what we have found so far seems to be similar to KairUs' starting point: most of the components, especially metals, never die. They not only live on and on after the smartphone's death, but they also already have a long history behind them before they enter the smartphone. As one of our interview partners, Rainer Bunge from the HSR Hochschule für Technik Rapperswil, puts it: "It is quite likely that a modern smartphone comprises at least a few atoms of copper originally mined during the Bronze Age." Focusing on the history of matters from this perspective, we realized that there are a lot of uses and misuses of a commodity and its components, which go far beyond the original intentions. For example, we saw a lot of migrants located at the cheap border shopping center trying to repair smartphones and making a living by selling electronic parts. They are no hackers or circuit benders, and the repair options are restricted due to the glued parts, but they try to make a living with something others depict as waste. Their agency is similar to the people surviving in Agbogbloshie, showing us another, more artifactual perspective in this entire issue, far away from the usual euphoric recycling discourse referring to the smartphone as a mini-mine. For there are always losses, but at the same time the material cannot be erased from earth. Destruction happens by mixture, and the components of a smartphone are mixed by definition. Furthermore, it is exactly the modern machines in the recycling centers that mix the matters instead of

disassembling them like the African or Indian recyclers do. "Waste," said Bernd-Stefan Grewe in our workshop, "is matter that is too much mixed." It is matter that you can no longer separate into its valuable components, at least not in an economically sensible way, or that you cannot grasp, because it is too fluid or too small.

We developed a sustainability ranking for electronic items, since we feel that looking at the recycling process only is narrowing down the whole problem in a non-feasible way. Looking at the use of electronic devices as a whole must, first of all, include the question of sufficiency: Do we really need this item? Even the best-practice recycled electronic item still needs material and energy for its production and recycling will never be performed for 100% of the material. The next point is the average time the device is used: phenomena like "planned obsolescence" are really counterproductive in this context. In places 3 to 5 in the ranking are "reuse of the whole object", "repair of the whole object", and "recycling of still usable components as a whole". Only after this stage does the regular recycling industry come into action, which is still preferable to the controlled burning of the material for energy production. At the end of the sustainability ranking we placed "legal landfilling" and "uncontrolled dumping" at the very end. The important point is to really understand that recycling is only a part of reducing the whole ecologic impact of electronic devices.

Thus, a lot of waste never disappears, it is nowhere and everywhere. Nanosilver is one more example of a metal that never dies, which is why we want to pursue it. It is nano particles made from silver; they are able to penetrate bacteria and other microorganism, and are expected to be widely used in consumer products that have something to do with cleaning: They purify smelly socks, for instance. Like the surface of the smartphone, this aspect is the clean side. On its other, dark side, they not only will never ever disappear, but they may also intrude and transform necessary microorganisms to a yet unknown level, because they are made to transform or kill the unwanted. They are agents of matter, no living organisms. Beyond its "zombie" (Jussi Parikka) aspect, it is this dark and

uncontrollable side of our cult of purity that interests us. All these considerations will end with our third object, "urban mining", which is more a question of handling objects than an object itself. In other words, the object is the city as a mine, the process of reclaiming compounds and elements from buildings, streets and sediments. Consequently, all that is built and constructed, is a mine. It can be taken or hacked or reused in manifold ways.

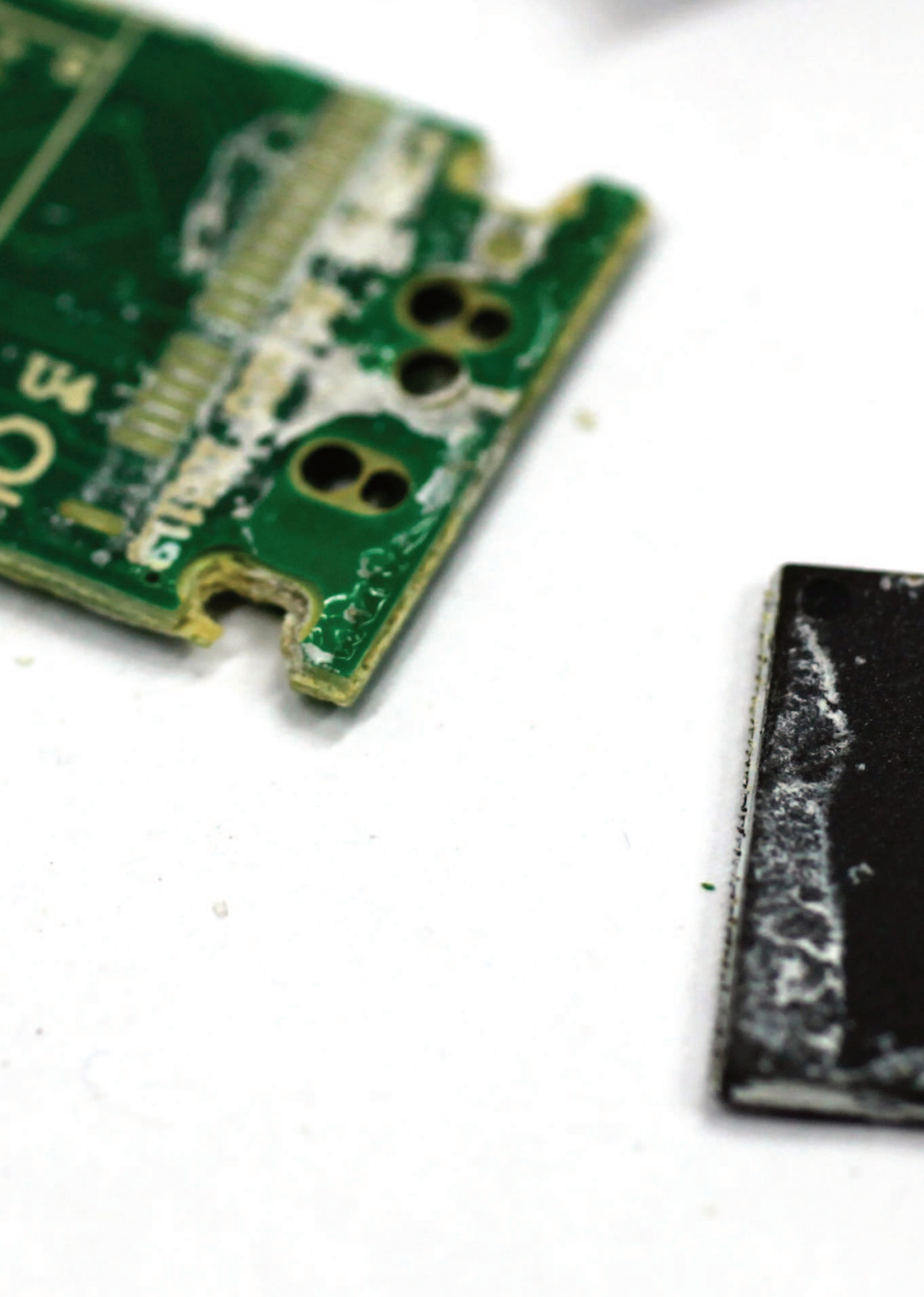
ECOLOGICAL THOUGHTS ABOUT OUR MODES OF COLLABORATION

Our research team is interdisciplinary, consisting of a core team of six people ranging from visual anthropology, environmental studies, art theory, scenography to music and programming. During the first year, we worked quite closely together on the concept and the research. This intense phase of working in the core team was something very special. We shared what we found during our own investigations, and spent hours in discussion, trying to understand what we were doing. Sometimes we also conducted the field work together, e.g. interviewing experts. Maybe it had to do with the complexity of the subject. This is different from the initial phase in "RhyCycling", where we separated and began to work in small teams much earlier, opening up to interventions from "outside" – by the ones not belonging to the subteams. Now it seems that we have reached this point too. We are building smaller teams for the realization of the audiowalk, the digital archive, the object biographies, etc. The teams include people who want to work more closely together or who share a common interest, have the needed skills, a professional background. And we are beginning to include our project partners more intensely – ranging from scientists in the humanities or ecology to NGOs and the local government and from the exhibition context.

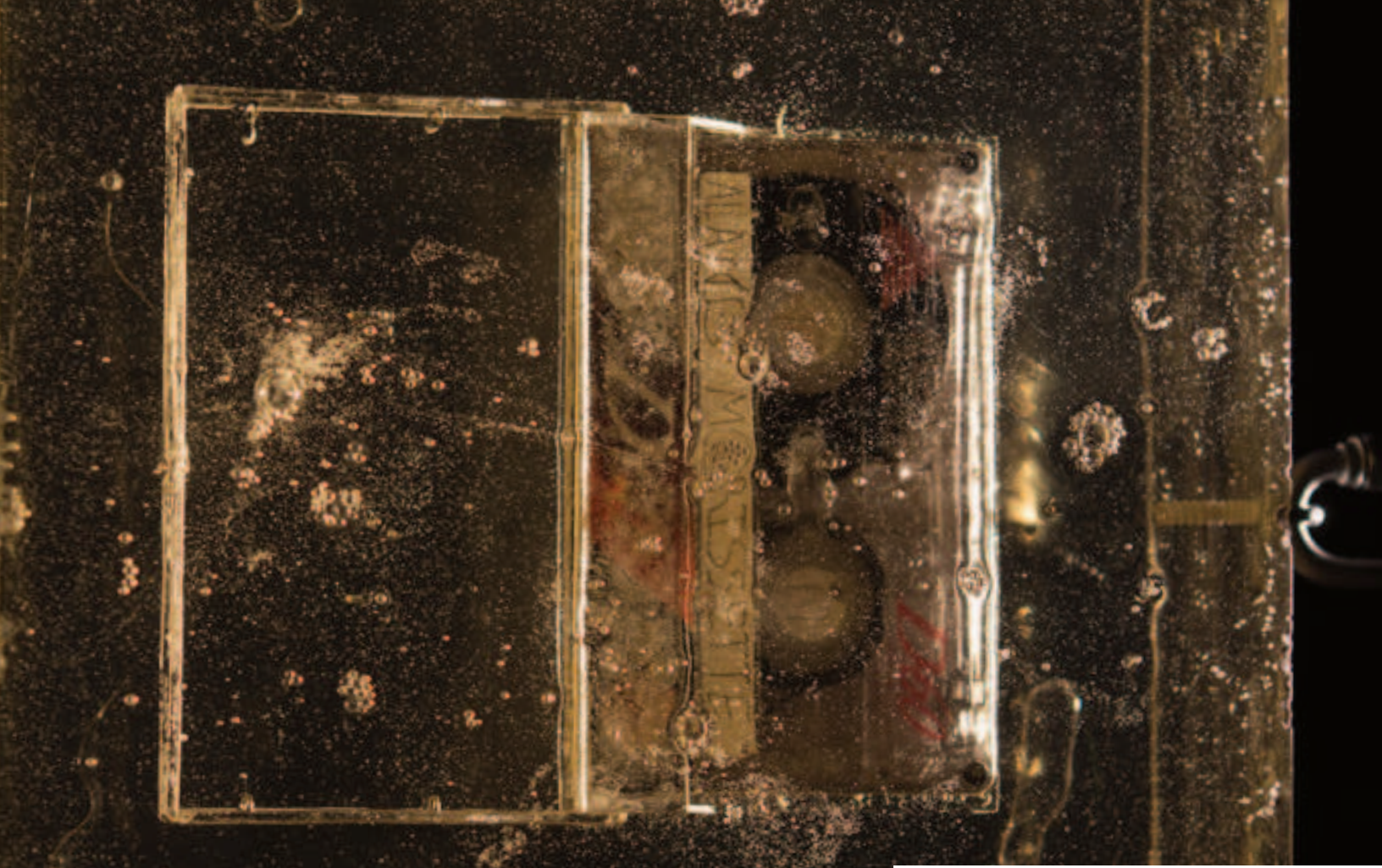
The inter- and transdisciplinarity in our core team functions primarily as different perspectives and inputs. Without our environmental scientist, for example, we wouldn't be able to perceive "hot" topics, like the rare earth elements or the nano-silver issue. And she can tell us from a natural science perspective how things are interlinked. But we not only gain expert knowledge from one another, we also learn to listen to each other, to deal with differences and various thinking patterns. Thus, although we are very different, we have to think of a common goal, and have to come to terms with each other. These are highly uncertain processes. But in reverse, it is the sharing of this process what lets us dissolve borders and generate joint outcomes. One problem of this process could be that we, as well as our outputs, are slowly assimilating, loosing the hard edges, becoming homogeneous. On the other hand, it leads to a multiplicity, because we have to accept that there are other points of view different from one's own. Tue Greenfort once said in a talk that ecology is about interdisciplinarity. Timothy Morton says that the ecological thought is about co-existence. We think that our mode of collaboration, of acting out and going through our differences and opening them up for interventions from afar, is in that sense: ecological.

Research team "Times of Waste"

The interdisciplinary research team consists of a core team of six people ranging from visual anthropology, environmental studies, art theory, scenography to music and programming: Flavia Caviezel (lead), Mirjam Bürgin, Anselm Caminada, Adrian Demleitner, Marion Mertens, Yvonne Volkart, associated: Andreas Simon. Most of the team members have been collaborating since "RhyCycling. Aesthetics of Sustainability in the Basel Border Area", 2010-2013; "Times of Waste" runs from 2015-2017. Both projects are situated at the Institute of Experimental Design and Media Cultures at the Academy of Art and Design of the University of Applied Sciences and Arts Northwestern Switzerland.
`http://www.ixdm.ch/portfolio/times-waste`.




.ne
.me
.quittes
.pas



DIGITAL DATA FUNERALS

Interview with Audrey Samson by Linda Kronman

Linda Kronman (LK): Your works *ne.me.quitte(s).pas* [1] (do not leave me) and *Goodnight Sweetheart* [2] can both be seen as digital data funerals and artistic strategies to deal with the deletion of data. Yet in your research you talk about the difficulties of deleting data, specially in the case of Facebook, Google and Twitter. How hard or easy is it to erase data once uploaded in the circulation of social media?

Audrey Samson (AS): Yes, both works are about erasing data, but as you say it is rather impossible, so in the works the gesture is very symbolic. How difficult is it to erase data? I think it is nearly impossible, especially online. When one's data is uploaded to the cloud, we normally don't know where the server is, and the only real way to destroy data, is by physically destroying the hardware, by de-magnetizing it or smashing it. Obviously you can't march over to Google somewhere in California and say – I would like to smash my section. And even if you could, because of how things are copied and propagated through the network, deleting data is practically impossible.

---

1 **ne.me.quitte(s).pas** is a ritual of erasure, a symbolic attempt to escape datafication. The starting point of the project is a public installation that offers USB keys and a set of instructions in a pre-addressed envelope. The audience that engages with the piece sends their data in the post to the artist. In a biochemistry lab a digital data funeral is then performed. The keys are immersed in a mix of acids called Aqua Regia, used to dissolve noble metals. After digestion, the remains are are sent back to the owner by post in a small jewelry box.

2 **Goodnight Sweetheart** is a funeral for digital footprints and identities. In this artwork USB keys and other storage devices are collected from participants and embalmed in resin, forever sealing the data.

LK: Another thing you have written about is issues of data ownership after a person's death. What are the current policies of the major social media platforms handling one's digital legacy after death?

AS: These policies change very quickly, so hopefully what I say is current, but it might be six months or a year old. For example Facebook recently implemented the 'Legacy Contact', which is not available in all countries yet, but definitely in the US and DK. If you have Facebook, in your profile settings you may designate the person who would be your legacy contact. This person may update your profile picture and add new friends, also download a copy of your Facebook data. You used to be able to choose whether your account should be deleted or memorialized (upon proof of death). But of course deleted is again a big word, because they don't really delete the data. Even if they delete your profile data, your ID still exists, and all your data still exist, shared through other peoples profiles.

LK: What happens in practice when the profile does not appear anymore? Will the persons be deleted from the friend lists etc.?

AS: This is very recent so there hasn't been much testing on it. So it should be that it takes you off all those lists. But in the past when profiles have been 'taken off', they have still appeared in e.g. birthday reminders. Or they have this new thing 'your memories', and this has been very troublesome for some people, because for example their dead brother appears in 'the memories' one morning, so there is this kind of ghost in the machine that lingers on.

With Google it is not really a death policy, they don't even use the word death, which is very interesting. It is the 'Inactive Account Manager'. So we get this idea that we never die online, we just go inactive. The 'Inactive Account Manager' is not for death per se, but it deals with inactivity, for example if you are in a state of health in which you can't deal with your accounts. So, you are able to determine what you do with all your Google things, such as Google Wallet, Gmail, Google Drive, and all the other million things we have there. But if you say you want to delete something, you are not erased from the server logs. You are supposed to be able to erase your search history, but actually you can't because it is saved in the server logs, so in that sense your history is just somewhere else.

Twitter does not really deal with death (apparently they would discontinue the account). Basically if you are dead, how would they find it out and how do they verify it? I am not sure how this works. There are so many services that will continue your twitter presence even after you die, so the whole idea of death does not seem to exist on Twitter.

LK: That is also interesting: how does a company really know a person is dead? They might just be inactive.

AS: On Facebook that was actually quite an issue. Because before the legacy contact one had to show proof that a person is dead, for example with a death certificate. But it appears that in practice this was not always verified. So it happened that someone said a person was dead and it was a prank, so the person's Facebook was de-activated, but the person was still alive. They then had to prove that they were still alive. So they got hacked in a way. This raises questions like: How do you prove that you are still alive, when there are so many modes of presence through bots and algorithms? What does it mean to be *alive* anymore?

LK: So in the end, if we want to erase our presence from Facebook, dead or alive, it is impossible?

AS: I think so, it is absolutely nearly impossible.

LK: In your work *ne.me.quitte(s).pas* USB sticks with data are physically destroyed by using acid. And in *Goodnight Sweetheart* various storage mediums are embalmed in epoxy, totally blocking the access to the data they contain. What was the process to choose these strategies of deletion for your artworks?

AS: I was thinking of ways to destroy data so that it could not be accessible anymore. Another more visceral way than just smashing the hard-drive with a hammer. Then I met Jonathan Kemp, who was making gold cocktails from old hardware. You can strip the heavy metals by using a specific mix of acids called 'aqua regia' (HNO_3+3 HCl). It is an old method to make gold soluble. I thought wow, gold cocktails, this is such a poetic drink. Learning about the process of the acid being able to dissolve the metal, that's when I thought – can we try this with the USB sticks? That is how the whole thing came about, through collaboration with him.

In the second iteration it became apparent that using the acid was kind of a cremation of the data. I don't know if you know someone who has been cremated? When you receive the ashes afterwards – it is very strange material thing to receive. It became clear that the remnants I would send back in the post, were like remnants from a cremation.

In the second project I thought what if we could embalm the data, make a relic out of it, in the way people embalm animals or humans at the funeral before burying them. The choice of the material came about for practical reasons; what can dry in such a way, in a certain time, that is transparent and that can have the embalming features. It ended up with resin for the devices and epoxy for the USB sticks.

LK: Both of your projects are also participatory. The data was chosen and given to you by the participants. Have you collected any statements of how they felt about the final erasure of the data?

AS: I have a little bit, and I must say that it is rather incidental in the sense that I never intended to ask people afterwards about the data. It was always supposed to be an anonymous thing. I never look at the data, I just either embalm or cremate it and send it back to them. Interestingly I have been reproached for this, apparently it is my duty to collect metadata about what I erase, people cannot let go. But I did end up doing interviews about the project, incidentally with people that had done it, so I do have those statements. And interestingly enough most of the people I spoke to had sent data relating to a past relationship. Not necessarily someone who died, usually a past boyfriend or girlfriend. So, for example you have old pictures in your pictures folders and every time you go looking for an image you might see an old photo of that boyfriend. These people would say that this gave them the opportunity to organize it in a way, to decide what to keep and what to delete, or just to erase everything, to get closure from that relationship. That was the story I encountered most often.

LK: The biological human memory needs to forget: How important do you think it is that in the digital realm there is a right to be forgotten as well? On the other hand when someone dies we want to remember them by creating monuments; how does this translate to the digital?

AS: That is a tough question. I think it is very important to be able to forget. Both in the human brain, if we can make such a separation anymore, and online. To be able to erase is definitely crucial to the eventual function of our collective memory. But that is not to say – erase everything; rather – how do we then think about archiving

in general? Archiving is always a power structure, so whoever gets to decide what we erase, is also the one who has the power to decide such things. I was thinking recently about how it could be in the future, that you might have to pay to have things erased. The people in control of the servers would have the ability to erase data and it would be a very high-cost service. So the rich people would be able to delete their data and the poor people would not.

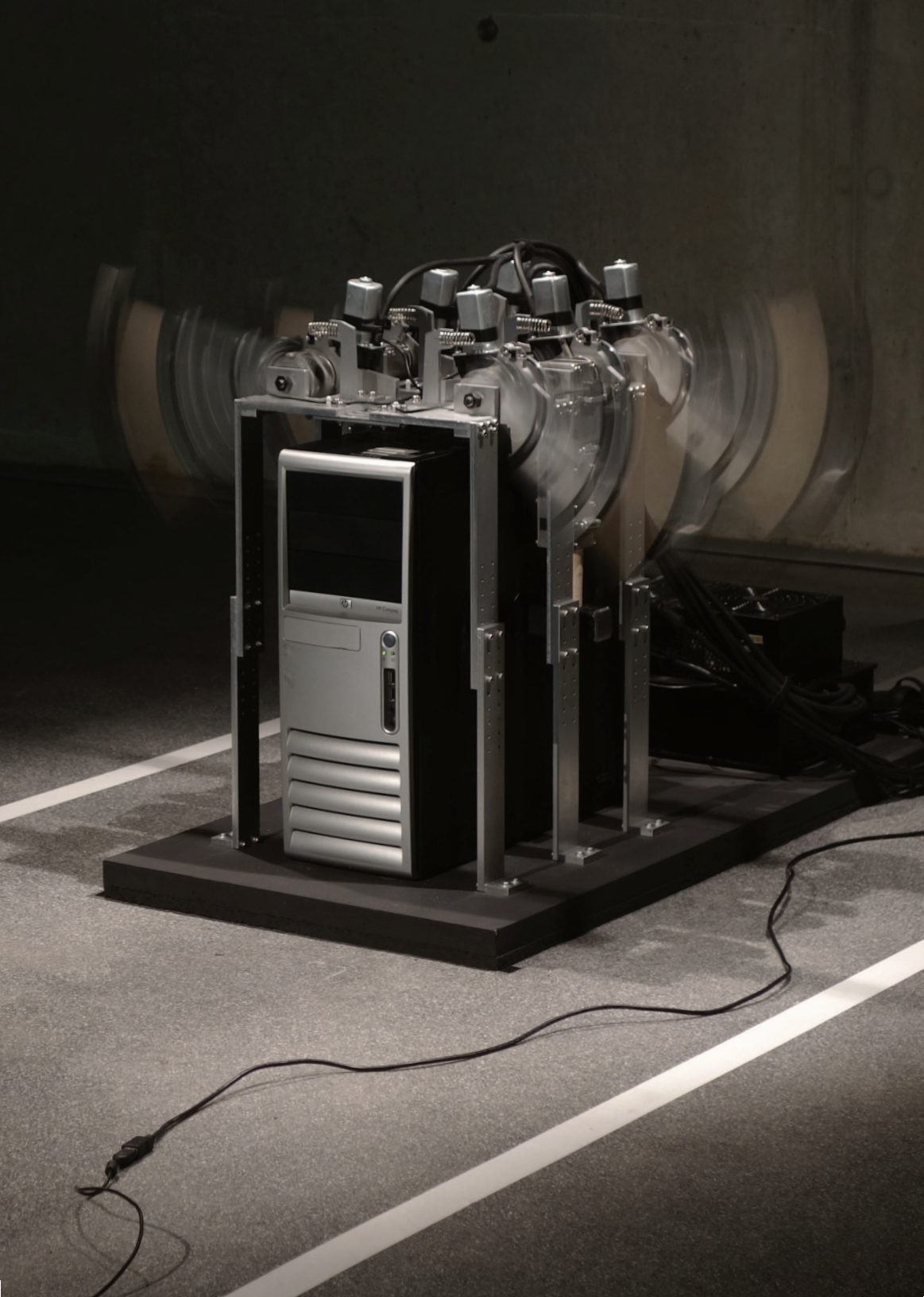
LK: This is very interesting, because today one is ready to pay for recovering lost data, so why not pay for deleting data? It sounds like a very evil business model!

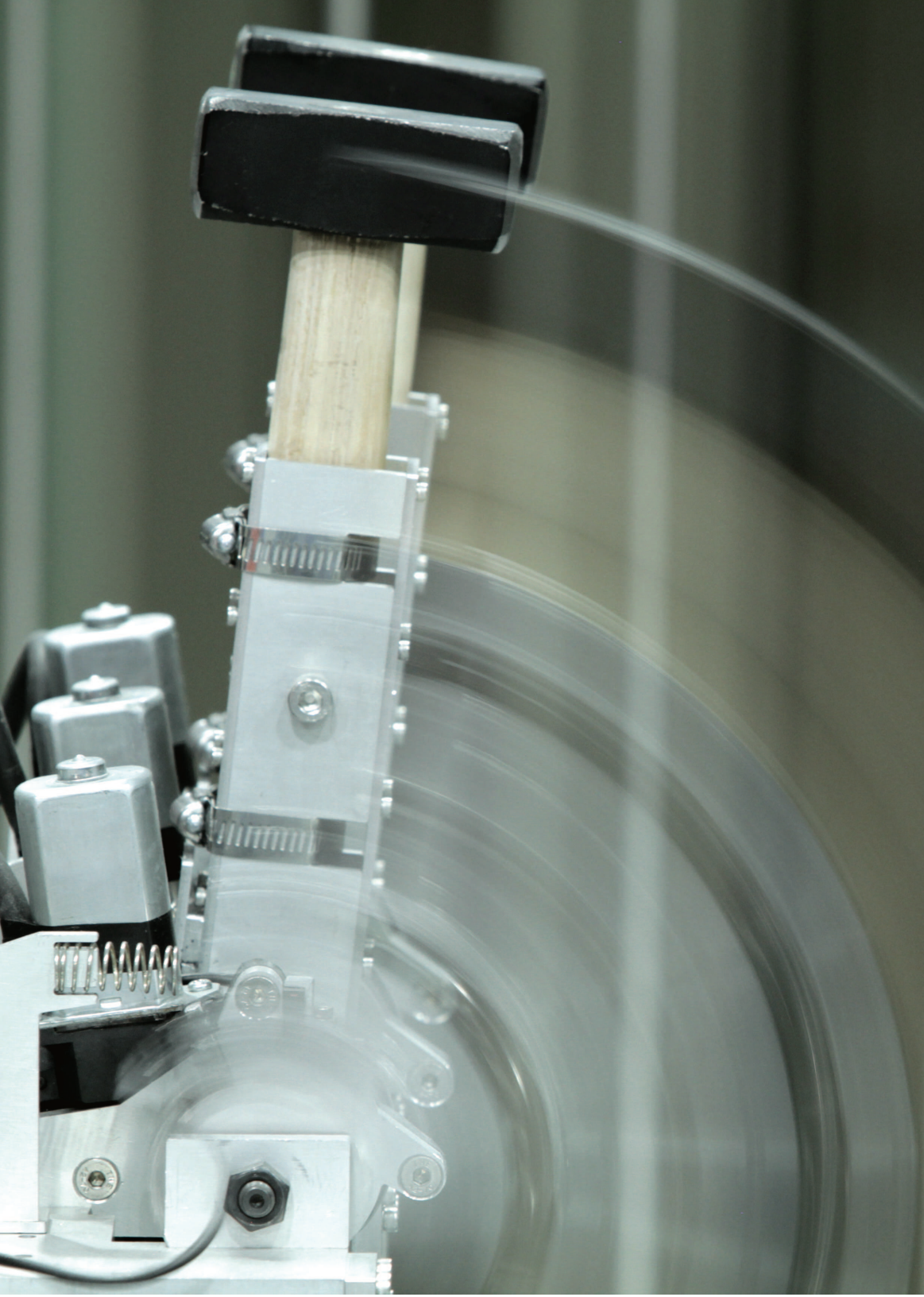
AS: It does, but I think it is not such a far-fetched idea. It started a long time ago, that when we get free services, all of what we do online is tracked, even when we pay it is tracked. All this information we give involuntarily to the company. Now there are services that will specifically ask you for more personal information, for example tracking your heartbeat, and then you get the service for free. We are already starting to see the digital divide between people that have no money at all, that will just give away whatever information asked to obtain a service. I can see this building towards the point where there is all this evidence that can be used against you, as we know, and you should pay a big price to get it erased.

LK: As a last question, do you think there can be artistic strategies to deal with this?

AS: I think that artists working with strategies of deletion or erasure are addressing the issues. Thinking about networked data as part of our selves, and therefore treating it in a different way, as a material thing with consequences, that will help us to deal with these issues. Artists that work with erasure of data emphasize materiality of data, and this is very relevant. Demystifying the ephemeral cloud network fallacy will already change how we address these issues.

Audrey Samson (CA) is an artist-researcher currently completing a PhD at the School of Creative Media in Hong Kong. Her performative installations explore how memory and technical objects are iteratively reconfigured and entangled in the context of networked data archiving. Her artistic approach, informed by the cultural context of technology, is ethnographical and rooted in software studies. Samson's work has been presented at festivals and galleries throughout the Asia Pacific, Europe, and Canada.





TECHNOLOGY-BASED ART AND DESTRUCTION – EXHIBITING MALFUNCTIONS

by Stefan Tiefengraber

Easy, uncomplicated interaction with interactive art installations and an entertaining approach to attract visitors opens up room to learn the story behind the art. These are the main goals of my projects and a big part of the two introduced works *User Generated Server Destruction* [1] and *your unerasable text* [2]. Both works invite visitors to destroy something. One time a text message is printed out and shredded, and the other time it is the destruction of a server by the force of hammers. The two installations are available for 24 hours each and can also be operated by users not in the venue, creating an independence of opening hours. While *your unerasable text* is displayed in a shop window (depending on the exhibition venue), *User Generated Server Destruction* can be followed via a webcam, which is part of the installation. The server is filmed and viewable via stream on a website specifically created for that purpose.

Both installations are easy to interact with. *your unerasable text* is operated by short messages and *User Generated Server Destruction* provides three buttons on the website to push. Behind this surface of fun and interactivity, the user is invited to question the background of these technologies. Why do the pieces work this way? What data is generated? Who has access to it? Where is the data?

---

1 User generated Server destruction, www.ugsd.net
2 Your unerasable text, www.stefantiefengraber.com/yourunerasabletext.php

USER GENERATED
SERVER DESTRUCTION – 2013

Visitors of the website www.ugsd.net can trigger six hammers and drop them onto a server that is located in the exhibition. This server hosts the website, a single site that shows three buttons to release the hammers and a video stream to follow what's happening with the piece. The installation ends, once the server is destroyed and can therefore no longer host the website.

If you are connected and looking at a website like this, it seems to appear out of nothing. But there is data – zeros and ones compiling an image, text or a video. It is tempting to think there is no physical connection to any hardware. The physical, sculptural attendance of the work *User Generated Server Destruction* typifies the coincidence of the virtual, the intangible world of data, and the physical world, where we, the humans, exist. The installation visualizes very directly that behind the virtuality that we attribute to the data on the Internet, there actually is tangible reality and actual physical hardware.

The Internet is a continually growing network of servers spread all over the world. On the one side are the users and on the other side the suppliers of the network. Usually, it is only possible for computer viruses and very qualified users to attack and destroy highly protected servers that are locked in well secured places.

These places are data centers, where the big 'Data-Farmers' are saving all the information we are providing them with. Looking like factories, these centers have big tube systems to cool all the computers. They are strategically built near rivers, guaranteeing enough water for this process. You will always find a power plant

close to it, feeding electricity to computers, which are not only hungry for data but also for electrical power. Highest standards of security protect the data from loss by any means. The risk of losing the data is not to be taken, no matter how important the data is. One never knows for what or whom it might be useful for some day.

As users we can control our computers and are able to easily destroy hard drives. But the data we feed to clouds and websites is impossible for us to control and erase. Spread over many hard drives and servers across the world, there is no access for us. *User Generated Server Destruction* poses a counterpart to this. It is something that works in the other direction and hands the power back to the users, who are all of a sudden in a position to decide freely what happens to the data. It becomes possible to erase one of the servers and thereby shrink the worldwide network for the blink of an eye. What is left is a sculpture created by destruction, typifying the physical presence of the Internet.

So far, 27 servers in several exhibitions all over the world have been destroyed. Although employing similar hardware every time, it took from 2 to 1002 hits for the hammers to finish the destruction. Some servers stopped working after a short period of operating and some worked for several days, although being hit permanently. For some curators this is hard to exhibit, since the installation can be destroyed at any time, leaving a non-functioning artwork behind. That creates a fear of disappointed visitors, not able to participate in the process of destruction. Given the common notion that an interactive artwork has to function non-stop, this is difficult.

The concept is to destroy the server and only leave a sculpture and a video documentation behind, archiving the process. The server is not supposed to be fake, and there is no intention to make it more robust than it initially is. This would make the artwork weaker. Each server receives an individual, ascending number, and the hits are displayed on the website for every server in one exhibition. Nevertheless, replacing the server after destruction makes the piece more interesting for galleries and museums. A solution for longer exhibitions, like the one in the Ars Electronica Center in 2013, which lasted around three months, is to only operate the server during a certain time of a day. The server will be active 24 hours, but the time of operation is limited.

At the Node festival in 2015, the curators agreed to just show one server and host a "launch event" following an artist talk. This provides the time to generate curiosity and create attention, as everyone wants to have the first, and maybe already final, hit on the server. A lot of people waited to finally hear the sound of the 800 grams heavy sledgehammers smashing the metal cover of the computer.

YOUR UNERASABLE TEXT - 2011/12

your unerasable text is an interactive installation dealing with the topics of data storage and elimination. The installation can be placed in an exhibition, but is ideally exhibited in a window in public space, where it can be used by people passing by 24h a day.

The participant is asked to send a text message to the number written on a sign next to the installation: "send your unerasable text message to +43 664 1788374"

The receiving mobile phone transfers the data to a computer, which layouts the message automatically. It is then printed on to a DIN A6 paper, falling directly into a paper shredder. There, the message remains readable for a few moments and is then destroyed. The shredded paper forms a visible heap of paper on the floor, growing with every message.

your unerasable text works via SMS, as it is the easiest and most comfortable way for the participant – and almost everybody owns a mobile phone. The standard for the short message service was implemented in the early 1990s and is still used and integrated in every mobile phone, even in smart phones. Another advantage is that users don't have to be close to the installation, messages can be sent from all over the world, and they don't need any additional software or access to the Internet to participate.

When *your unerasable text* is used, the sent text message isn't erased. The data is passing by the mobile carrier of the sender and receiver, the mobile that is integrated in the installation and the computer processing the text and sending it to the printer. At each of these points the data can be saved. The installation stores a file of each message consisting of the sent text, the phone number of the sender, and time and date when it was sent. The only thing that actually is erased, is the print, which is just a visualization having no effect on the data itself.

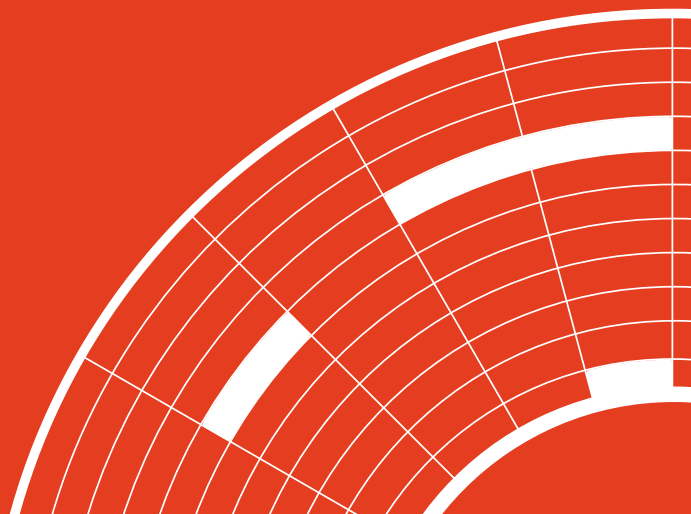
The storing of data is a rather current topic, given the discussions on bringing back the "Vorratsdatenspeicherung" (data preservation) in Germany, along with discussions in the Austrian parliament about passing the "Staatsschutzgesetz" (state protection law) including points to bring back the previously overturned "Vorratsdatenspeicherung", under the guise of this new law.

Also very recently, the Safe Harbor law was declared illegal by the Court of Justice of the European Union, creating the need for re-negotiation between the EU and the US to change this law.

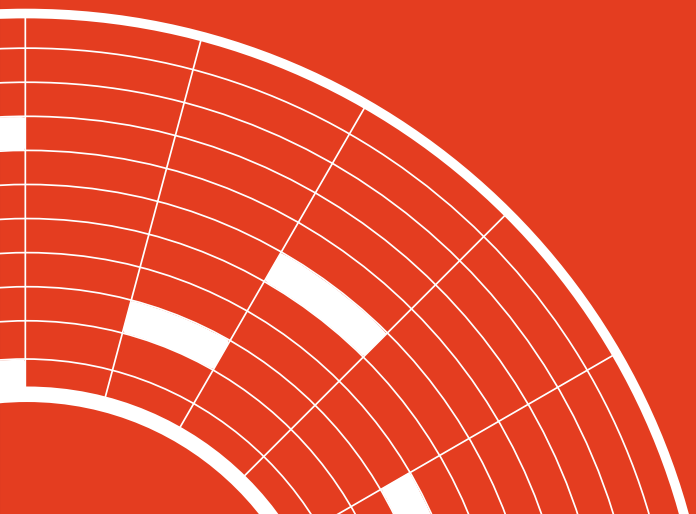
This also raises questions about the locations of the servers we are using and the law applied to the data stored on hard-drives all over the world. There has to be a definition of who legally has access to our data and is able to pass our information on to third parties. This is also a significant topic in the installation *User Generated Server Destruction*.

As far as exhibitions and other possibilities for exhibiting these works are concerned, maintenance is a crucial point. Both installations have a high frequency of usage, 27 servers have already been shown and destroyed in 10 exhibitions. By November 2015 more then 27.400 short messages were collected.

Stefan Tiefengraber's (AT) artworks go from performances to interactive installations to sound art and time based media such as experimental video and documentaries. These works have been exhibited at Ars Electronica Festival 2014 (Linz/Austria), O'NewWall Gallery (Seoul/Korea), 16th Media Art Biennale WRO 2015 (Wroclaw/Poland), …



RE SURF ACING DATA



Third Person Data

by Dr. Michael Sonntag

What is “Third Person Data”?

Data about a person may exist at various locations: if we think about our own personal data, e.g. our preferences in communication (who we send E-mails to or receive from), interests (what we “like” on Facebook) or habits (which websites we visit regularly), then many persons know about these things. Obviously we know about ourselves quite a lot (but take care: you might be able to name your favorite E-Mail contacts, but could you correctly identify all topical areas you “liked” in the past?). Comparatively easy to identify are persons or corporations we gave the data to directly: our E-Mail provider, the social networking platform, and the websites we visit regularly. We might not always like that they know, but this is difficult to avoid and data protection laws provide not only theoretical but at least partly also effective limits and remedies against data misuse.

Much more difficult to “take care” of are third persons processing our data: not only would you have to know about their existence and what they actually collect and store, but they can also be located anywhere and you do not have any contract with them – or they would not be third persons. Examples of such third persons and third person data are:

- **Advertisement networks:** They place advertisements on various websites. Through their own cookies they track users across all websites where one of their ads is displayed. Note that the owner's influence is limited to the advertisement area – everything else is under direct control of the advertiser and cannot be hindered or prevented by the site. If at one place they can identify the person (e.g. through login and data sharing by the website operator), then all collected data from all sites can be attributed to this person.

- **Intelligence agencies:** Monitoring Internet lines, especially at the backbone level, allows collecting data on many users and in detail. Even encryption only partially helps, as e.g. the IP address (source computer and destination web server, for instance) cannot be hidden in that way. The only advantage for users is that the amount of data is so large that only small parts can be stored for a longer time: complete data is collected only in case you are individually targeted (for whatever reason).

- **Platform participants:** Platforms like Facebook, eBay, or Amazon know you, which is obvious. Not immediately apparent is that many elements on these platforms, e.g. products, games, or additional services, might be provided by third parties. While their name is often accessible or even shown, they may collect significant data on a user's behavior or interests without clearly appearing as someone else: they look like an integral part of the platform. Often they can access data other than that which directly collected in their "parts" through the platform, e.g. the user profile or parts thereof. Typically default privacy configurations allows extensive access.

- **Identity providers:** Logging in through a single central account may be simple and convenient, but simultaneously the identity provider can collect a list of when the person has authenticated where. Additional information may be disclosed too, e.g. if different verification levels exist or if the site where authentication is performed provides details like where in the site authentication is requested, for instance creating a new account, checking out, or performing specific actions requiring enhanced verification. These are third parties only in respect to logins; they may collect additional data directly as well.

- **Video surveillance:** Whenever you walk through a city, you will be recorded by video cameras. These could either be officially installed and operated e.g. by the police, or be privately used (but still covering public or semi-public locations – e.g. streets or shops). Usually there is no direct information at all regarding who collects data, storage duration, who has access to it when, etc. Each camera alone is typically not very interesting, but if the data of many is combined and becomes available, the person can be identified (e.g. by facial recognition, detailed accounts of the locations a person visits when). Another example for gathering data are automated toll collection systems and section controls. Most operate by license plate recognition, which works very reliably on a technical level. Also, in some countries such systems are built into tow trucks driving through cities and scanning for cars suitable for repossession. Naturally most of the license plates scanned will be useless, but technically there is no problem at all storing this information in a database, associated with a timestamp and a geolocation, for future use (building profiles, selling etc).

- **Storage reuse:** Old data media might be securely erased or destroyed, but very often that is not the case and they end up on auction websites as “used/second hand”, or through shops as “refurbished”. Sometimes they are shipped to third-world countries for recycling or disposal. In all these cases data on the media may remain accessible, because with modern harddisks, for example, securely erasing the content but leaving it in working order is complicated and requires a long time. For other mediums (like SSDs or memory sticks) this may be even more complicated. Hence the data may end up somewhere else, although it has officially been destroyed – it is just that nobody actually took care of this. While targeted attacks are not possible, the results can be problematic for those unlucky persons whose data can be recovered.

- **Second persons “Plus”:** Even those we do have a contract with or freely give data to might change to third persons. When data is aggregated with other information (e.g. statistical data), used for a different purpose or passed on to someone else, the lines become blurred. Is this still the original data we gave to them? Who now physically controls it? What are they going to do with it? What if the recipient of data passes it on again – will you ever know who now has your data and what it will be used for? The end result therefore closely resembles the situation when a third party collects data itself.

- **Data theft:** Hacking systems is not fun anymore but business. Therefore data stolen from large websites is a valuable commodity and will be used and resold. Many times this takes place without the affected persons knowing this fact, as such hacks/data thefts are denied and kept secret as long as possible: admitting them would cause bad press, liability and increased security measures in the future for the company they were entrusted to.

Third person data can therefore be defined as data about a person which is stored, collected, or used by someone the person does not know is doing this (a third person), and where therefore no direct control or verification/supervision is possible.

Implications for Computer Forensics

For computer forensics, which can be roughly defined as the investigation of digital data in the context of legal proceedings, third person data can be invaluable, but also very problematic. Invaluable because this is data collected by someone who is not involved and therefore trustworthy. The suspect might have deleted his browser history, but the advertisement network still knows where he has been when (at least partially). But it can be problematic as well, because by default (i.e. in most cases) the investigator does not know who might have such data in her possession, and if they do, how to obtain access to it. Additionally there is no guarantee that data exists, that it is complete, of good quality, reliable etc.

How to know data exists at all – and where

The first and most simple option is just to know who collects which data. While this is a good approach for experts and in narrow areas, this obviously cannot be a general solution. Still it should not be omitted as computer forensics is something only experts should perform and these might then know potential owners of additional data. Such knowledge can be obtained or expanded through investigations. If e-mails are of interest, for example, then the layperson will see the sender (“Sent” mailbox) and the recipient (“Inbox”) as those possessing data about the time of sending/receiving the mail. But experts know that additional header lines (normally not shown!) exist, creating a trace of servers the mail traversed on its way from source to destination. And every server appearing in there might (or should, unless it was not saved or already deleted) have some third person data referencing this mail and can therefore confirm or refute certain aspects about it. This means that investigations may uncover potential holders of additional data usable as evidence.

Another option to discover third person data is to perform the same activities as the person suspecting the existence of such data, but simultaneously and explicitly looking for any signs of surveillance or even employing tools actively scanning for them. This is suitable for open video monitoring, for example: normally we don’t notice any cameras, but when we explicitly look for them, they are easy to see. Hidden (or temporary: see tow truck example above) cameras are more difficult to catch, but with enough experience and diligence these might be discovered at least sometimes. Also wireless connections can be detected easily (but not necessarily their content), leading to processing

devices which might collect some data (or not). On the Internet this is easier, as it is trivial to monitor all network traffic of your computer in detail. When visiting a webpage it is then possible to identify where the computer connects to, what cookies it sends out and receives, etc. But passing data on by the server or changes between the original incident and the investigation (new advertisement partner) pose significant problems.

If such third parties collecting data have been hacked, their data might have been published on the Internet. Based on this information, it can be assumed what these (or similar) parties are observing. So if you are not part of the data disclosed, some conclusions can still be drawn. The Snowden disclosure can serve as an example here. The capabilities of one specific secret service have been published, but it must be assumed that similar services in other countries are mostly capable of the same actions. Additionally, it is possible to identify what someone else with comparable access might be able to do – and therefore probably is doing.

This leads to the next, and rather pessimistic, category: when someone possesses the technical capabilities to monitor and collect data, he will. This is not necessarily true, but at least in countries with weak privacy laws this must be assumed. There data will be collected just in case and quickly be sold to others, if they show interest and are willing to pay. So this approach is better suited to identifying what kind of data might be third party data than who the third party is.

Definite third party holders of data are all kinds of “upstream providers” of services. AirBnB does not own any servers, for example, instead they use Amazon web services. So Amazon obviously does have physical access to all of their data. They might not be allowed to look at it

(contract), but they can access it, e.g. in case of emergencies or on request of third parties. While direct data access seems unlikely, using the data for calculating statistics is quite probable. Physical access is especially interesting if the company gets into financial difficulties, as Amazon might use their data as security, preventing any access by them or you, the actual owner, or as compensation for unpaid invoices (e.g. through selling to someone else; similar to utilizing domain names in bankruptcy).

The last useful option is inserting incorrect data and waiting for it to come up somewhere again. For instance an arbitrary e-mail address might be created and disclosed to a single provider (creating a new one for each target is not difficult). Whenever someone contacts you on this address, you know one person to whom your data (or at least parts of it) was disclosed too – and from which source. This is obviously time-consuming and works only if data usage is observable (e.g. difficult with video surveillance). Also, "storing for future use/reference" cannot be detected in this way.

Finally you could perform illegal actions where the only evidence is the potentially monitored behavior and wait to be arrested (which resembles the previous approach). While this method is very reliable, as the police/prosecutor will have to disclose how they found you and present the evidence in court at the latest (hence the behavior must be the only evidence existing at all), this cannot be recommended. Still it is useful regarding other persons (e.g. criminals performing illegal activities for other reasons), as verifying what has been used as evidence in the past can be assumed as a lower limit of what is possible today.

As an overview, the methods described above are presented here briefly in a table with some properties: time required to obtain information, reliability (wrongly assumed to possess data or incorrectly seen as having no data), completeness (will we find all such third parties) and associated costs (not necessarily monetary, but also effort required or “drawbacks” experienced).

Source of knowledge	Time required	Reliability	Completeness	Costs
Just know	None, but long preparation	Medium-Very good; depends on sources	Medium-Very good; depends on sources	Low; most sources are free
Do again and observe	Low/as long as the original	Good; wrong identification is unlikely	Medium; depends on observer	Low
Third party sources	None, but long preparation	Medium; disclosed data is correct, mere reports not necessarily	Low; only what actually occured and was published	Low-Medium; many sources are free
Technical capabilities	Medium; investigation who + capabilities required	Low; not everyone who can, actually does	Good, but not every party can be identified	Low
Upstream providers	Low	Good; services can be bought (=tested)	Low; often not disclosed	Low-Medium; depends on data provided/testing
Publish traps	Medium-Long	Very good; actual use is observed	Medium; depends on time and observability	Low-Medium; providing data is free, but active tests might cost
Illegal activity + wait	Medium; investigation will take some time	Very good	Very good; limited to certain groups (enforcement)	Very high

Obtaining access to third-person data

If somebody wants to know what a third person knows about them, several options exist. However, it must be considered that this party might possess the data illegally (or exceeding legal permissions) or are simply not interested in disclosing this fact (only bad press, but no additional revenue). Therefore replies may be slow or non-existing. From the computer forensic view, at least in “official” cases, e.g. court proceedings, several additional options do exist. Moreover, cooperation of the data holder might then be enforceable (at least within a country).

First, the person can request access to her/his own data. This only works for personal data according to privacy laws, explicitly granting this right. Outside the EU, someone possessing data because of a contract is not necessarily required to provide it. This situation is very problematic with third parties, as they are usually unwilling to disclose it voluntarily. Also, while the person might have a contract with company A, and this company a contract with company B, this does not automatically mean that data at B must be disclosed to the person. Any court case is between the person and A, for example, so B is an “innocent bystander” and unaffected by these proceedings. Only A might be ordered to rely on some contract provisions it has with B to first obtain data and secondly disclose it. This requires the person to at least conclusively demonstrate that such data probably does exist and would help the case. Even then, especially in civil proceedings, access might be difficult, as B could argue that this would adversely impact trade secrets. Only in case of criminal proceedings is such transitive disclosure easier, because the police can also search/impound data located at third parties (after obtaining appropriate permissions, typically from a judge).

Indirectly this third person data might be obtained through information from the second party: what is stored there could have been passed on to third parties, and, if logs are available, the actual transfers might be reconstructed as well. While this seems to establish an “upper limit” (at most these items could have been

transferred), that is not the case. The third party may have obtained separate additional data from other sources, combined it with such other information, or enriched it with previously anonymous data. So in reality, more or more detailed information may exist with the third party. Still this approach serves as a first approximation.

An illegal method to obtain access is hacking the data custodian. This could be the actual owner or someone else, e.g. a cloud provider, with physical access. While this is obviously illegal, in case of sufficient knowledge/resources, it is a quite promising method. Advantageous is that no owner consent is required and that internationality is not a problem but rather a boon. However, hacking is typically not that easy and there is no guarantee of success. Often only a webserver can be compromised and other servers, where third-party data might be expected, are more difficult to reach.

As third-party data is only rarely collected for the purpose of merely owning it, but rather for deriving monetary benefits, offering to buy it is another chance for retrieval. It might be necessary to pose as someone else (typically a company intending to use the data), as well as to obtain a larger part of the dataset (e.g. all Austrian users). This may obviously be costly and/or illegal, especially if data of other persons must be acquired too or false statements (“I am a company”) are involved.

Problems of third-person data

While the person the data is about typically desires access to it and simultaneously wants to keep it secret (i.e. the owner of the data should not be allowed to use it or pass it on further), this is not necessarily the case. Sometimes the owner would be interested in publishing the data, e.g. to be able to provide an alibi. This may contradict interests of the third party: data is only valuable if it is not generally available, and more so when its legality is questionable. But even if the person obtains the

data, owners might retain some rights to it, especially if the original data (collected or received) has been enhanced or combined with data collected by them. This is comparable to the problem of credit-worthiness checks: while data access is granted (and the person could then publish it), the algorithm for calculating the score remains secret and need not be disclosed. Additional persons might be involved too, such as telephone call records, which can create further difficulties: any party might obtain access, but publication must consider rights of other communication participants too.

While third person data can be difficult to access legally for the persons affected, this is not equally true for data owners – collecting or buying it is legal in many jurisdictions. Even then – and more so when ownership is not perfectly legal – such data is typically kept "secret". So knowing about it becomes difficult, reducing the acceptance of such data by the persons affected. However, this effect should not be overestimated. Considering the existing public registers of applications using/storing personal data (mandatory within the EU), little effect on the general population is observable, which rarely even knows of their existence. From this it can be concluded that public registers or general availability of data categories stored by someone are unlikely to significantly improve the situation. And individual rights to retrieve such information would be enough for e.g. investigative journalists.

Legally, third person data is difficult to regulate: by definition there exists no direct contact or contract between data subject and data owner. Therefore all rights of both parties depend either on the law or a chain of contracts, which might be enforceable by third parties – or not (legally possible, but restricted in scope and difficult in practice). Combined with the typical internationality of electronic data this further complicates matters, as normal contracts are much easier to enforce across borders than such contract chains. Also, national laws obviously differ and then the only hope are the EU or international treaties: harmonized rules applying to many countries. The problem of international relations in personal data was recently tackled by

the ECJ, who ruled that “Safe Harbor” provisions allowing the export of personal data to the USA are invalid. Another example is that the collection and export of personal data might be illegal in the “source” country, but gathering and importing it can be perfectly legal in the “destination” country. While in “real” life such trans-border situations are hardly applicable (using a telescope to watch persons across borders), this is the typical situation on the Internet.

Another issue of third person data is correctness: how does someone (i.e. the person it is attributed to, but similarly the third party itself) know, whether data is correct or not? It could lack important details, contain old values now invalid, or include calculated data which was correct enough for the original purpose but is not for the new one. Also, third person data might just be invented. An example for the latter are fake profiles identified in the Ashley-Madison website hack. While it is unlikely that names/e-mail addresses of real persons have been used, e.g. for pictures or other data, often actual profiles are harvested from other dating websites or scraped from social media platforms. Re-identification could therefore lead to real persons, for whom it can be difficult to explain that it was not them using a fake name and an anonymous e-mail account. Verification of third person data is complicated by the fact that it was not obtained from the persons directly, so modifications or additions might have been introduced at any intermediary point the data passed through – typically without information where exactly. Another source for incorrectness or inconsistencies is that such data is often collected solely indirectly (i.e. not through asking the person but observing and drawing conclusions). For instance devices might be shared (especially common with PCs and tablets, which the whole family might use; less so mobile phones), but any data collected through it is attributed to the “one and only” owner. For instance, when a father allows his children to use his tablet they might contact their friends, e.g. through chats, visiting social media profiles, posting messages and so on. Therefore obviously this adult male is strangely interested in small children, contacts them, and must be a pedophile in the eyes of someone observing

data only indirectly, e.g. through trackers in advertisements. Such danger is much higher for third-parties, as they typically do not interact directly with the person they are collecting data about and therefore have few chances for noticing a different user, for instance, as in the example.

When considering the difficulties of deleting e.g. revenge porn or any other data from the Internet, it becomes clear, that the existence of third person data is problematic. This is exemplified by the possibility of “removing” data from Google search results. The data itself remains on the Internet, is still indexed, will continue to show up in search results etc – only searches for “name” or “name + topic” will not contain this specific link (searches for “topic” will!). In relation to Google this is again third person data, and while rendering it a bit more difficult to find is commendable, this cannot be considered a real solution. Either the data needs to (or may) remain publicly accessible, or it should be deleted. Otherwise we create classes of people: those who possess the tools or the knowledge to find things, and the “dumb masses” who do not. The latter will then have no control over their own data and not be able to find it, while the “privileged” can access all data (their own and others), therefore creating an artificial distinction and partial immunity, as they can hide their misdeeds, while others cannot.

Outlook

Third person data will increase in the future, as much more data is being collected and will be retained. And what is stored will be used and transferred on to maximize profit. Especially problematic in this context is the “Internet of Things”, where many small devices are equipped with computing power and communication possibilities. Here easily even the vendor could become a third party – no permanent contract is really needed for a coffee machine, but “outsourcing the evaluation of the data to the cloud for better brewing of coffee” is going to be a reality: see for instance Nest thermostats, which send a lot of information

to the cloud in the hope of slightly improving comfort or reducing heating costs (where energy savings might be offset by the additional energy required for communication and cloud servers!). Who exactly receives this data and what is or will be done with it later remains unclear. Regarding future developments, similar considerations apply to cars (mandatory eCall: an automatic telephone call is placed to an emergency number in case of a crash; a continuous mobile phone connection is optional for this application, but added-value services are envisaged – then a third party, the mobile phone operator, will be able to continuously locate any car, at least if in use), or fitness trackers (e.g. sending data to health insurance companies for lower payments).

What options exist to improve the situation or reduce problems? Some approaches could be:

- **Transparency:** Publication of who possesses which data, perhaps with automated abilities to check whether you are included. Based on past experience, only few people would actually use such a system. On the other hand it is complicated and expensive to set up and could easily open up security holes, allowing other persons access to such data (effectively spreading data out even more!).

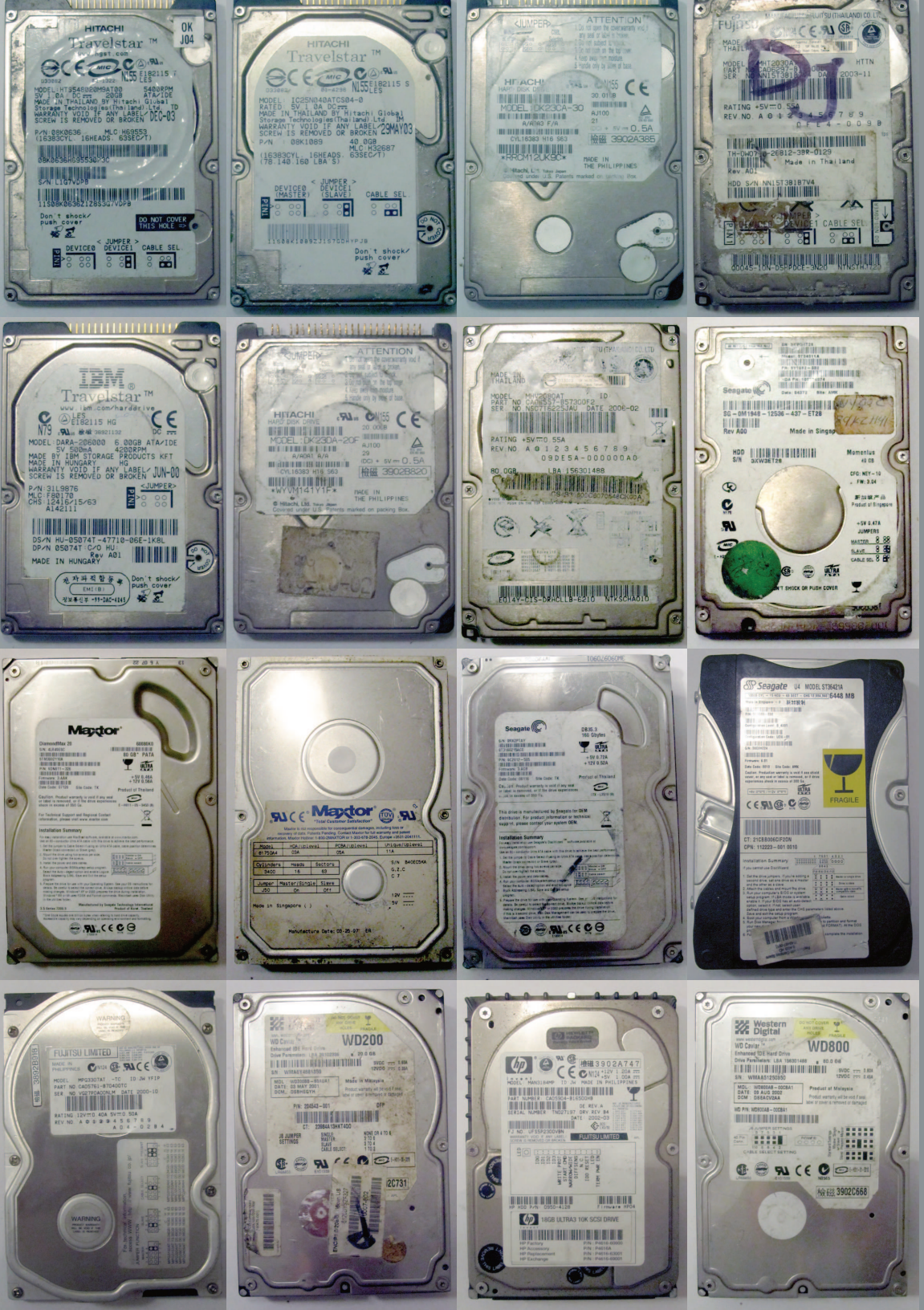
- **Legal regulations:** Restricting third party data and allowing it only in specific exceptional cases or when obtaining the data from the person directly (i.e. only direct data but no third party data). This seems unlikely and difficult to monitor, but should not be ruled out completely. Most business models on the Internet depend on directly collecting data and then “selling” it. While actually selling it would become difficult, limited, or forbidden, this would still allow “renting” it through placing targeted advertisements on the same site. Aggregation with data from other sites or independent sources, however, would be problematic.

- **Restricted disclosure:** Probably the most effective solution is to restrict the amount of data passed on to others. As soon as someone else knows it, restricting its further distribution is becoming ever more difficult through internationality, electronic communication, and data sharing. Therefore everyone should carefully select whom to disclose what data to. Is the person trustworthy? What will she do with the data? Whom will she pass it on to? As a supplement, gathering data should be regulated more tightly, as secretly gathering data reduces such "data autonomy". Verification is difficult, but as soon as someone knows about the existence of data, the onus would be on the data owner to prove direct collection instead of receiving it from someone else.

- **Extended deletion rights:** Whenever someone controls data which is not explicitly allowed by law (e.g. public registers) or a contract, the affected person could have an unequivocal right of deletion, independent of the interests of the data owner. So whenever the existence of data becomes public, everyone could request deletion of their data – regardless of whether it was acquired legally or not. This would, however, require effective supervision to ensure such deletion actually takes place. Closely related would be mandatory "data decay", i.e. mandatory deletion after some time has elapsed, unless the data has been "re-acquired" in the meantime.

Mag. Dipl.-Ing. Dr. Michael Sonntag (AT) is associate professor at the Johannes Kepler University in Linz at the Institute for Networks and Security. He studied both computer science and law and is researching and teaching in the areas of smart home and web security, computer forensics, and IT law. In addition to the Universities of Linz and Graz, he also regularly teaches at the ELTE in Budapest and the University of Economics in Prague.


Shift


HITACHI
Travelstar
OK
J04
HITACHI
Travelstar
ATTENTION
FUJITSU
IBM
Travelstar
Seagate
Maxtor
Seagate
Western Digital
WD200
WD800
FUJITSU LIMITED
18GB ULTRA3 10K SCSI DRIVE

BEHIND THE SMART WORLD ARTLAB – ARTISTIC STRATEGIES FOR DEALING WITH RESURFACING DATA

by KairUs - Linda Kronman and Andreas Zingerle

> Breaches of Western information security thanks to a rise in electronic waste circulation have been particularly pronounced in Ghana, where a certain cadre of citizens has taken to searching out information on Westerners' old hard drives for extortive purposes. [1]

Since 2010 we as KairUs artist duo have focused on researching topics such as spam, scam and Internet fraud. In August 2014 our research had evolved to the stage that we needed to take a field trip to West Africa, where a considerable number of so called advance fee fraud originates. Rather than hunting down scammers in Internet cafés, we were interested to see which technological affordances or limitations the scammers were faced with in this part of the world. In our initial research we came across reports about an electronic waste dump called Agbogbloshie. In the middle of Ghana's capital Accra, in this toxic wasteland by a lagoon, is where our electronics from developed countries are illegally dumped. Jennifer Garbys examines in her book *Digital Rubbish* [2] in detail how electronic waste ends up at e-waste dumps such as Agbogbloshie; first they linger in

---

1 Jason Warner, Understanding Cyber-Crime in Ghana: A View from Below, 2011 International Journal of Cyber Criminology (IJCC) ISSN:0974 – 2891 Jan – July 2011, Vol 5 (1): p. 736–749.

2 Jennifer Garbys. *Digital Rubbish: a natural history of electronics*. USA: University of Michigan Press, 2011

storage, from there high-grade machines might be resold, the dysfunctional machines are then shipped in containers to harbors in developing countries such as the one in Tema, where most of the e-waste enters Ghana. In Tema the containers are sold and transported to Agbogbloshie. The next step is the salvaging of components, copper, gold, iron, plastic, and anything else of value.

Electronics are made of minerals and chemicals, natural resources that are gleaned by organic laboring bodies, no matter whether this takes place at an e-waste dump or in a mine. One of the most memorable sounds from Agbogbloshie was the clacking sound of metal scrap hitting the aluminum structures of a computer, when the workers were disassembling the computers into mother boards, processors and hard drives and further for extraction of valuable metals and raw earth minerals. Components and materials salvaged at Agbogbloshie enter new cycles of production, reentering the consumption cycle, whereas the residues remain. Moore's Law, a near golden law within the world of computing, predicted the computer revolution in which the rate of innovation within electronics has decreased to as little as 18 months.[3] Creating something new will thus be followed by an another gadget turning old. These old electronics, dead media, or zombie media, as Jussi Parikka, names them leave fossilized traces of designed obsolescence and gadget-culture.[4] At Agbogbloshie these materials are difficult to recycle; the toxic, unstable materials mix with the black ashes of burned cables and pieces of electronic fossils. They pile in indefinitely growing layers of obsolete technologies, if not directly washed through the lagoon into the sea, as we witnessed during a day of heavy rain. This is how: "*dead media creeps back as dangerous toxins into the soil or then as zombie media recycled into new assemblies*"[5]. Agbogbloshie, our electronic dystopia earned its nickname - Sodom and Gomorrah.

---

[3] Garbys, *Digital Rubbish: a natural history of electronics* → p.30
[4] Jussi Parikka. *A Geology of Media*. University of Minnesota Press, 2015 → p.60
[5] ibid. → p.60

Among other components, *"zombie"* hard drives also enter a new chain of value available at Agbogbloshie in stock for a negotiated price. Likewise the data saved on these storage media resurface, even if they were dumped in the trash, both physically and metaphorically, in the bin on our computer desktop with an expectation of permanent deletion. What took us to Agbogbloshie in the first place were reports we read on how journalism students had discovered data breaches of companies and governments when recovering data from hard drives bought at the e-waste dump. [6] Additionally we found articles describing how scammers abused data originating from hard drives collected at e-waste dumps in West Africa. [7] Therefore, when visiting Agbogbloshie we decided to buy twenty-two hard drives, curious to see whether dumped data would persist, and could it easily be recovered and would it be of potential value? Could the data be artistically reused and/or rather easily abused?

When we returned to Linz our plan was to follow media theorist Jussi Parikka's suggestion:

> In the age of consumer electronics, the artist can also be thought of as an archaeological circuit bender and hacker, which links media archeology with the political agenda of contemporary media production. [8]

Our plan was therefore to recover the data from the hard drives and offer the data and the hard drives as source material for artistic production. During two DIY-data recovery sessions we accessed data from three hard drives, just by plugging them in to a computer. This means that the data on the hard drives was not even deleted. Two

---

[6] Emily Chung, B.C. students buy sensitive U.S. defence data for $40 in Africa, CBC News Posted: Jun 23, 2009, available at: `http://www.cbc.ca/news/technology/b-c-students-buy-sensitive-u-s-defence-data-for-40-in-africa-1.803353`

[7] Jason Warner. "Understanding Cyber-Crime in Ghana: A View from Below". In: *International Journal of Cyber Criminology* (2011)

[8] Parikka, *A Geology of Media* → p.150

hard drives were recovered by trying out open source tools such as PhotoRec, TestDisc and Partition Magic. In these cases the data was deleted by the owner, by trashing it into the "bin" or using the delete command. We learned that deleting data is a rather symbolic gesture, whereas the data is not actually deleted until it is overwritten. According to data specialists, even overwritten data can be recovered with special tools [9] and the only hundred percent secure way to delete data is to physically destroy the plate where the data is stored. This was demonstrated in one of the "stranger episodes in the history of digital-age journalism", when the Guardian had to destroy all their hard drive copies of NSA files leaked by Edward Snowden. [10] What made the episode strange was that British authorities supervising the erasure of the data as well as the journalist were all aware of existing copies in America and Brazil, proving that the strength of digital data to persist is in the easiness of duplicating it.

Of our twenty-two hard drives, seventeen were physically damaged. In this case such parts as the internal read write heads or the spindle motor can be changed and the data can still be recovered. The complicated part is to get the spare parts, as each brand and model use customized parts, which can still vary depending on the manufacturing country. Therefore we asked for help from the company ECS-solutions that recovers lost data as a business model. Even with their help only one additional hard drive was recovered. This was mainly because the hard drives where relatively old, with production dates ranging from 1997-2008, and spare parts were not easily available.

---

[9] https://en.wikipedia.org/wiki/Data_erasure#Full_disk_overwriting

[10] Julian Borger, NSA files: why the Guardian in London destroyed hard drives of leaked files, the guardian.com Aug 20, 2013, available at: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london

With 85 GB (229.446 items) of recovered data from six hard drives we approached nine European artists with various artistic practices, inviting them to use the data and the hard drives as a source for creating artworks. In May 2015 we met for an extended weekend to discuss ideas and our approaches to the recovered data during the "Behind the Smart World" ArtLab. Considerations raised during the ArtLab led to discussions about ownership of data, how to deal with abstraction of data, how to avoid exposing private individuals without their consent, and the labor of structuring data that mostly consisted of "junk" such as porn, system files, and images downloaded while shopping online. Browsing through the recovered hard drives, it became rather obvious that as a consequence of seemingly unlimited data storage, we hoard rather than collect data. Rather fast it became a laborious task to get an overview of what just a couple of hard drives contain, specially when recovered data lack both filenames and structure.

During the weekend we also invited experts in data recovery, data forensics, and data policies to support us in developing strategies to deal with the data. Additionally, a visit to a recycling center gave us to better understanding of the material aspects of electronic waste.

As an outcome of the ArtLab we developed strategies for dealing with the data, which developed into concepts and further to artworks for an exhibition. There were two main approaches that emerged from the ArtLab, one of them focusing on the recovered data and the other exploring the material aspects of the physical hard drives. We became aware early on that using data from a hard drive as found footage needed a different approach than photographs, film or video cassettes found in a box at a flea-market. Our data forensics expert Dr. Michael Sonntag suggested that we should mix data to avoid accidentally exposing a person's identity. Another approach was to transform the data, mapping it to another format, which is the case with Joakim Blattmann's artwork, in which metadata and

folder structures from the hard drives are mapped to a musical score for a classical piano. Metadata can expose surprisingly private information and folder structures are like personal memory paths. As a soundscape certain patterns can still be revealed, while by abstracting the source we avoid exposing any private data.

Fabian Kühfuss's work *Shopimation* examines how rather impersonal images downloaded in our browser cache during online shopping can bring us closer to an unknown individual and his or her "aesthetic dreams". *Shopimation* uses thumbnails to build up a subjective code of an aesthetic, thereby translating the very private dream of who the owner of the hard drive would like to be. This work echoes the economic ecologies of our commodified Internet experiences, in which our profiles, interests and desires are continuously tracked and used to accelerate our consumption.

Emöke Bada's *Virus Chart*, on the other hand, looks at the trackers, the malware and viruses – the unwanted intruders on our hard drives. As the artist explains in an e-mail:

> Before even starting to look at any of the files, I followed the standard procedure of running a virus scan. Which was interesting because at the end of the day, on the harddrives that have been recovered so far, there were 881 viruses all in all.** [11]

Earlier viruses and malware were often destructive, even causing physical damage to the host, while today's digital parasites hoard data and are most successful as long as they are not recognized. The *Virus Chart* takes a close look on the "health" of these hard drives using medical charts as a metaphor to describe their maleficent content. Could it also be that the "poor health" of the hard drives was the reason why they ended up at Agbogbloshie in the first place?

---

[11] Emöke Bada, personal e-mail communication Jun 4, 2015

In a trilogy of installations, we as the artist duo KairUs returned to our initial research questions of what is the value of the data on a hard drive and how could it potentially be (ab)used? We know that dealing with data is a rather lucrative business today, yet as we learned from our data policies expert Fieke Jansen, the data of one person is worth only 0.7-0.01USD (a speculative estimate made by dividing Google's value by its users). In these terms data points are only valuable when connected to others, revealing patterns and desires. Selling the content of a hard drive to data brokers is worth less than selling its spare parts to a company in the data recovery business. What can make a hard drive valuable, on the other hand, is sensitive personal data that can be abused, including access to banking or shopping accounts, private images for blackmailing and harassment, or identity theft. This was the case with U.S. Congressman Robert Wexler. He was contacted and blackmailed with information from one of his discarded hard drives that was found in a second-hand computer market in Ghana.[12] By using DIY-data forensic methods combined with open source intelligent strategies and tools, it was also possible for us to confirm one of the owners of a hard drive with sensitive images. And another hard drive shows evidence of being used for romance scams. The potential abusing of data is therefore the focal point of these works, illustrating a number of "worst case scenarios" based on the recovered data. Even if there is nothing to hide, your deleted data might still return to haunt you.

Shifting to the works that deal with the material aspects of the hard drives, Michael Wirthig's *Inside Data (The Forgotten)* focuses on the drive platter as the actual physical container of our data on a hard drive. This experimental film travels through the inner parts of a hard drive in extreme close-ups, using light field microscope images to give the viewer an intimate perspective of the rather impersonal

---

[12] Warner, "Understanding Cyber-Crime in Ghana: A View from Below"

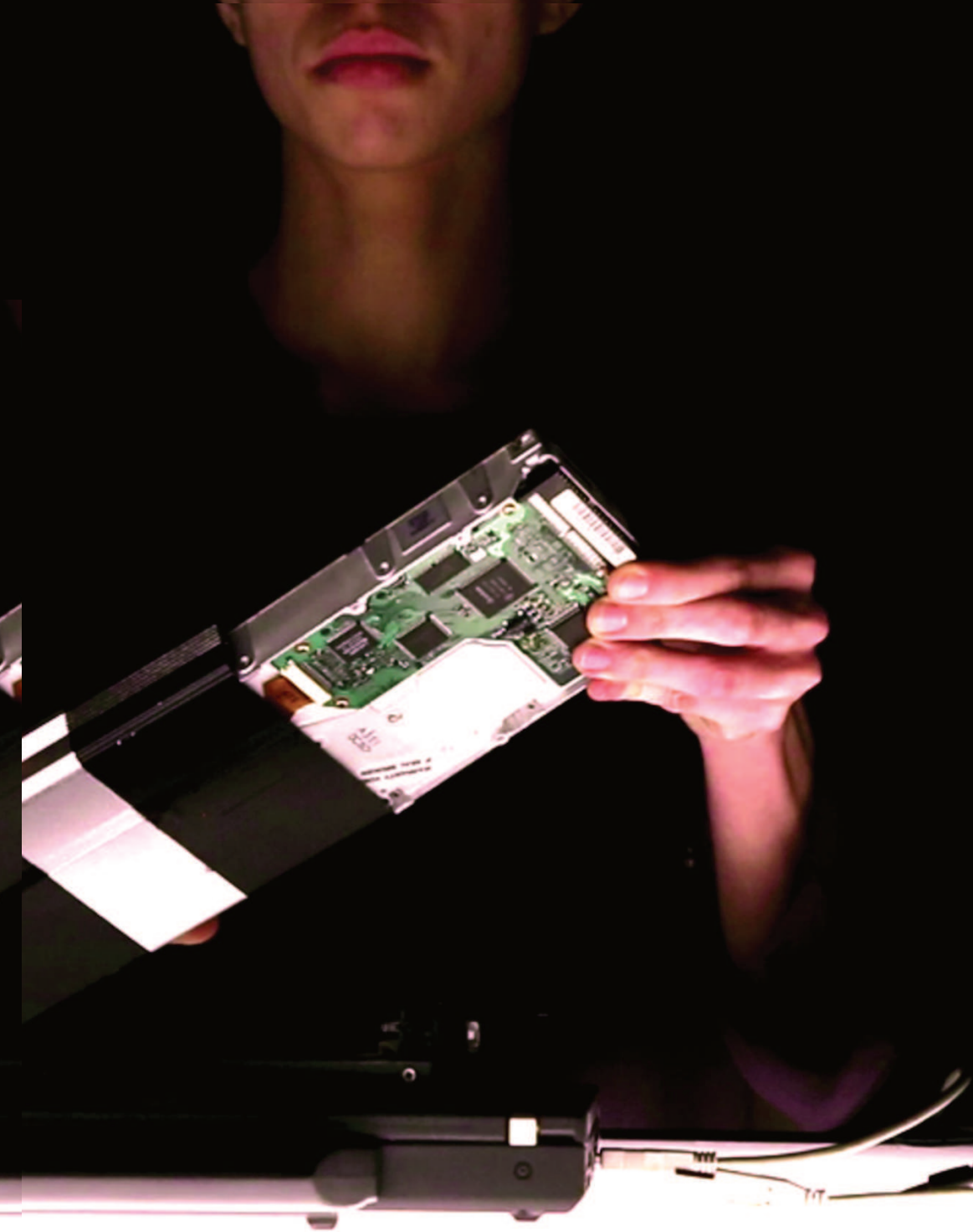
metal plate. Scratches and dust are made visible, the most common physical damage to our hard drives and most often the reason for these devices to fail. As it was impossible to recover the data from the majority of the hard drives brought back from Ghana, this work investigates the most fragile parts of digital data storage.

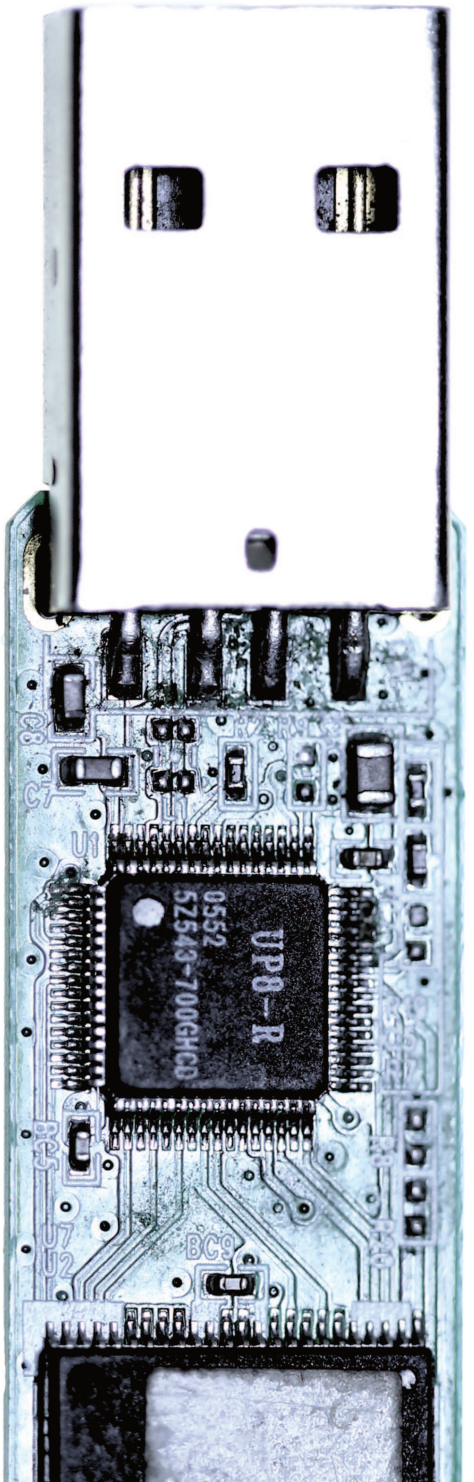
From a forensic perspective, which rests on individualization, each hard drive is unique. When zooming in enough with a magnetic force microscope, even *"individual bit representations deposit discreet legible trails"* [13], forcing us to review our perspective on the illusion of an immaterial bit just as a symbol either as a 1 or a 0. Also Simon Krenn's and Mathias Urban's work *Transposon* deals with the material aspects of data and storage media. During the ArtLab the artists collected magnetic field recordings from the hard drives, and when the sounds were amplified the experiment revealed that each hard drive has a unique sound. In the *Transposon* sound installation, the sounds are further recorded to wax cylinders via a modified Edison GEM phonograph, the earliest commercial medium to record and reproduce sound. The recordings are in this way reversely migrated from one "zombie medium" to another and further back to be mixed and listened to again in a digital format. Each migration brings further qualities to the sound, which is transformed along with the migration processes. Likewise, when any data is migrated, even in the case of digital files loss, corruption and glitches appear. These obsolete media with about a decade of age difference are the black boxes we as artists are called on to hack, bend and re-purpose, in order to critically reflect on our current relationship to electronics, their life cycles and residues. The twenty-two hard drives brought back from Agbogbloshie functioned as vehicle to discuss data privacy, data collection, data forensics, e-waste, erasure of data, and dead media. Behind the shiny smart world of advertisers, another reality is revealed, unfolding the consequences of our datafied consumer culture, which is far from being sustainable or fair.

---

[13] Matthew G. Kirschenbaum, Mechanisms: New Media and the Forensic Imagination (Cambridge, Massachusetts, USA: The MIT Press, 2012, paperback edition), p. 10.

KairUs is a collective of two artists **Linda Kronman** (FI) and **Andreas Zingerle** (AT). Our work focuses on human computer and computer mediated human-human interaction with a special interest in transmedia and interactive storytelling. Since 2010 we have worked with the theme of Internet fraud and online scams, constantly shifting our focus and therefore approaching the theme from a number of perspectives, such as data security, data privacy, ethics of vigilante communities, narratives of scam e-mails, and technologies in relation to fraud.




UPD-R
0552
SZ543-700GHC0

DELETED FILE INFORMATION IS LIKE A FOSSIL . . .

Interview with Michaela Lakova by Andreas Zingerle

Andreas Zingerle (AZ): In your practice based research project *DEL? No, wait!REW* you contextualize the process of data recovery in a forensic approach to a collection of discarded hard drives. In the installation, the audience is asked to either delete a recovered file or to publish it online. Can you tell a little bit more about this work? Where did you get the hard drives from? Can you describe the installation setup?

Michaela Lakova (ML): The installation *DELETE?No, wait!REWIND* aims to explore the notion of "deletion", confronting the audience with larger questions of how to secure deletion of data from a magnetic medium, data ownership and the ethics of data recovery.

The installation setup consists of three core elements: display screens showing the graphical user interface (GUI); a tangible physical interface, or controller; and a spatial element – a lit table top, which acts as one of two light sources. A spinning hard drive is connected to Display Screen No. 1, which shows the data recovery process in real time using open source software (testdisk). A cold steel controller reminiscent of an industrial machine is placed at the center. The controller has two buttons: Delete and Save. Delete provides the option to permanently remove a file from the system; Save uploads the file online. Display Screen No. 2 highlights a custom written software, which facilitates user interaction by communicating with the controller. Once the save option is chosen, the retrieved file is saved on a remote server and published in an online gallery. Saved files are projected on Display Screen No. 3. The physicality of the hard drives, the source of the data recovery procedure, is present in the exhibition space.

AZ: Were there any reactions from the audience? If so, what kind of feedback did you receive?

ML: People are sensitive about their personal data, but they lack technological knowledge about the structuring, storing and deletion of their electronic data. Often the viewers associate themselves with the actual owner(s) of the hard drives, who remain unknown. In that sense the installation achieved a greater awareness, which in some cases makes participants rethink the fallibility of technology and what happens when they trash their hard drives or files into their digital recycle bins.

AZ: Your work calls the ownership of the data into question. It raises questions like: Who actually owns that data? Is the creator, the audience, or are you the owner of the data? How do you reflect on these questions?

ML: The notion of ownership is polemic. The work is highly confrontational. It creates a moral dilemma. On one hand I became the owner by purchasing a collection of hard drives with a legal transaction. So the physical carrier and the accompanying content become mine in a sense. Then I am passing my ethical question(s) to the audience by given them a temporary ownership or control over the content. However, this is illusionary due to the fact that the recovered files have already been copied to software, and even when the delete button is pressed and the data has been deleted from that software, it still continues to exist on the magnetic disk, which is present in the exhibition space. Because of the slippery nature of the digital information, I think that the notion of ownership is blended out. In other words there are multiple owners of the same content.

AZ: In your work *Estimated Time to Recovery* you created an automatized system, which recovers and deletes files without the consent or the knowledge of the previous owners. What were the ideas you wanted to bring forth with this work? Can you reflect on the development phrase of the work and how you came up with the automatized installation format?

ML: The work proposes an insight to processes which often remain hidden and run in the background on our machines, *Estimated Time to Recovery* is an automatized system or a feedback loop of recovery and deletion as an attempt to display these processes, over which the users have no direct control. The installation consists of a metal box, which contains a mini computer Raspberry pi running open source software, which recovers and deletes data from a hard disk. The displayed numbers show the estimated time to recovery until the process is completed, and a screen, connected to the pi, shows recovered images in a random order. When the procedure is finished the machine starts the reverse process of erasing the recovered data. The choice to enclose all the hardware in a box is a metaphor of the black box of our general understanding of the machines.

AZ: If files are deleted and recovered over and over again, could you observe whether this affects the recovery or deletion? Do the images alter through the process, e.g. become glitchy or un-recoverable?

ML: *"Deleted file information is like a fossil – its skeleton may be missing a bone here or there, but the fossil remains, unchanged, until it is completely overwritten."*A beautiful quote from Dan Farmer and Wietse Venema, *Forensic-Discovery* serves for the purpose.

When images are restored they often inherit a sign of the recovery process – a distortion of the file, a glitch or an artifact which is present. While performing the recovery process over and over again, I was also prompted to identify corrupted files without any metadata, which could be assigned as "un-recovered". Their content was blank. This also caused some technical issues with my installation, so I decided to deliberately avoid them.

AZ: In the first installation you give the visitor a choice to delete or recover data, whereas in the second work the deletion and recovery process is automatized. Can you reflect on how this human interaction or lack of interaction changes the interpretation of the recovery and deletion processes?

ML: In the first work *DEL?No, wait!REW* installation, the viewer becomes an active participant, to whom a certain choice has been given, but this choice is still very much determined by an algorithm. In my second work *Estimated time to recovery*, on the other hand, the visitor becomes merely a witness of the process with no possibility for interaction. I think both of these roles resonate in our current media realm.

AZ: Another of your works is called *Cold Storage* and consists of enlarged transparent prints and five glass cubes that display the circuit boards. Can you tell a bit more about the work? Can you describe your research for the work and describe your aesthetic choices?

ML: The *Cold Storage* installation was made in the context of the group show entitled "What remains – Strategies of Saving and Deleting" at esc (medien kunst labor) in Graz. Together with four other artists I was invited to explore themes of storage, data, reliability, and the loss of materiality and values. I started my research by looking at

digital forensics and data erasure as main themes. However, the direction of my research shifted towards an investigation into data storage, macro chips, circuit boards, integrated circuit (IC) diodes, and the process of zooming into their macro structures. Eventually that was reflected in the final work and its aesthetics choices.

The installation consisted of enlarged transparent prints containing macro photos of the most common memory devices (USB stick, SD memory card and PC hard drive) which were placed in the windows of esc, inviting the passers-by to glimpse inside "What remains". Five glass cubes displaying the circuit boards (used for the photographs) were lit by a light box. The glass created an illusionary effect, which makes the hardware to disappear. Text labels (extracts from datasheets) are attached to each cube, informing the viewer of what they are looking at.

The idea behind *Cold Storage* was to investigate the architectural dimensions of our storage devices and how they are translated into the physical world. While digital storage becomes increasingly disembodied and dematerialized, hardware becomes more and more invisible, microprocessors and components become smaller and smaller, and chips are designed to be uncrackable. The work proposes a poetic overview of the material quality of memory, asking what is the future of digital storage? Is it *"a glass cold memory which lasts forever"*or an imperfect storage technology that can impart its contents?

AZ: So far in your works the owner is always separated and distant from the data rather than involved in a participatory act. Is this a direction you plan to continue or what are your upcoming steps in your research?

ML: In most of the cases is quite difficult to trace back the original owner(s). But even then I am not interested in personifying that data, which might center my works around the relationship with the actual owner. Instead, I try to keep it open for different interpretations. My next step is producing a small publication, based on my research and the collection of thoughts and images I have gathered.

AZ: So based on your research and your artworks, did this process make you more sensitive about how you handle data, or how do you deal with your data both on- and off line?

ML: I learned a lot throughout the research and the process, but there are still many technical aspects, which I do not fully understand. I am sensitive about my data, but I am also not super cautious about it. Otherwise I would have to become a monk. With this body of work I also attempt to showcase and discuss freely themes that interest me and might be of interest to others.

Michaela Lakova (BG) is a visual artist and researcher based in Rotterdam. Subjects of interest are errors, systems malfunction and the inevitable generation of data traces and its problematic resistance to deletion. Currently she is investigating digital forensics and the disappearance of hardware. She completed a Master's program in Media Design and Communication at Piet Zwart Institute in 2014.

NO GIVEN LOCATION

122

126

7

9

220

340

176


MEGACORP.

STRATEGIES OF NET-ACTIVISTS AGAINST PHISHING AND FAKE BUSINESS WEBSITES

by KairUs - Linda Kronman and Andreas Zingerle

This essay is part of our artistic research into vigilante online communities and Internet fraud. Online communities of so called scambaiters try to identify, block and report Internet crime activities. For this they have developed various strategies, ranging from creating warning platforms to collecting fake checks or blocking bank accounts, and they organize themselves in different forums.[1] One of these subgroups call themselves "Artists against 419" and host the biggest open-access database of fake websites. As of November 2015, there are over 4800 registered users and on average about 35 websites are added to the database each day. They use "passive reconnaissance" and "open source intelligence" (osint) tools to gather information, so that they can file reports to the hosting provider to get the websites taken off the web. Since 2007, the group members have discontinued using web programs such as "Lad Vampire" or "Muguito" to run "Denial of Service" attacks against the websites[2] and instead use online tools and written reports to maintain good relations with hosting providers and law enforcement[3]. In the following paragraphs we want to present one of their work-flow strategies to track and report fake websites.

---

1 Zingerle, Andreas and Linda Kronman. "Humiliating Entertainment or Social Activism: Analyzing Scambaiting Strategies Against Online Advance Fee Fraud." in *Cyberworlds* (CW), 2013 International Conference on. IEEE, 2013, pp. 352-355.

2 Brenner, Susan W. "Private-public sector cooperation in combating cybercrime: In search of a model." *J. Int'l Com. L. & Tech.* 2 (2007): 58.

3 Cain, Patrick. "Scam trap." *The Toronto Star,* `http://www.` *thestar. com, referenced March* 21 (2004): 2011.

Scambaiters use various vernacular tools and social engineering techniques in order to run background checks on suspicious business websites. Open source intelligence (osint) refers to intelligence that has been derived from publicly available sources both on- and offline. These tools are used in "ethical passive reconnaissance[4]" to gather as much information about the target as possible. In this version, passive reconnaissance is perpetrated by activists and hacktivists who are trying to gain information that will support their political causes or other such ethical motivations. Law enforcement officials may also use passive reconnaissance as part of a criminal investigation. Ethical or not, passive reconnaissance is always done without the authorization of the person or organization that is being targeted.[5]

This leads to an effective combination of classical social engineering attacks on the target, which in turn can be used to harvest more information. The following chapter summarizes the hands-on part of a workshop called "Credible fictions – Deceptive realities"[6]. In the workshop the *Megacorp.* installation served as a point of departure to further investigate Internet activism, resurfacing fake websites and osint tools. The online tools were presented to the group of participants, who gathered and discussed information using the collaborative writing tool "piratepad".

As an example website we want to focus on www.start-office.biz. According to their website, start-office.biz is an international company specializing in organizing virtual offices. They are located at the Wienerberg Twin Towers in Vienna, Austria, and currently offer jobs to local agents who should "provide relevant information online

---

4 Glassman, Michael, and Min Ju Kang. "Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT)." *Computers in Human Behavior* 28 (2012): 673-682.

5 Bansal, Akanksha, and Monika Arora. "Ethical Hacking and Social Security." *Radix International Journal of Research in Social Science* 1, no. 11 (2012).

6 "Credible Fiction – Deceptive Realities" Workshop notes: `http://www.andreaszingerle.com/credible-fictions-deceptive-realities/`

for direct clients and other relevant stakeholders through through popular social networking sites". In the following paragraphs, we will use the osint tools to analyze the website and raise suspicion about the legitimacy of the website.

LOOK AND FEEL

Every website is designed differently. Over the years certain trends in usability set standards for web designers. You can always ask yourself, how coherent is the web design? Does a photo with the company logo have a pixelated, poor quality, whereas all other photos are crisp and sharp? Does the logo look badly manipulated into an image?

On the front page of our example website we see the dark black logo of start-office.biz. Font type and size of the logo look misplaced and don't fit the overall dominant gray and dark blue color combination. In one of the header images the logo is clearly squeezed in the image. The company's headquarter is supposedly located in Vienna, Austria. The website claims to operate on a global scale and runs hundreds of offices in the USA and Canada. The page language is English and there is no translation to German available. On the "testimonials" page we find a review from a person called 'Michel' from France, who refers positively to a different company:

> Sunex's virtual office allows me to service these clients from anywhere in the world, while maintaining a presence in Texas.

So it seems that this review was copied from another website and the company's name was not changed. The "career" page offers an application form to apply for the "local agent" position. The salary is stated in USD and is paid on a weekly basis, which is also a very uncommon practice in Austria.

CROSSLINKS

You can check how many other websites link to your targeted website. In search engines like Google or Waybackmachine, type "link: www.start-office.biz" or use online search tools like backlinkwatch to figure out how many websites link to your website in question. Both tools report no backlinks. It is not a criminal act to have no websites linking to your website, but it still looks suspicious, when a page claims to be a global player and no customers link to them.

CONTACT INFORMATION

Every page has to provide a possibility to contact the website owner. Is the contact email the same as the domain name, or is it a free-to-use webmail service. Is the postal address a valid address? This can easily be checked through online streetmap services. Also phone numbers can be checked to see whether the area code belongs to a local number or if it is part of a call forwarding program. What happens when you call the number? Is the line in use during office hours?

In our example the company's address is the Twin Towers in Vienna, although it doesn't provide a floor number. The phone number has the correct country code "+43" for Austria and "1" as a city code for Vienna. A quick search in the local online telephone database ensures that the telephone number is registered at the state telecommunication company A1, but there is no name entry to be found.

There are two email addresses on the website: support@start-office.biz and hr@start-office.biz. An alter ego personality contacted both addresses and claimed to be looking for a job in Vienna. A person called Thomas Anderson replied as a representative of the company,

sent me his Skype account details and three pdfs that I should read through, fill out and return in time. The three documents included an application for employment, a confidentiality agreement and a job offer signed by a Michael Adams, Director of Start-Office.biz. By using an IP tracker it is possible to analyze the email header and obtain the IP address from where the email was sent. In case of the email from Michael Adams, the email provider is Telmex Colombia S.a. in Barranquilla, Colombia.

IMPRINT

Depending on the country in which the company operates, a trade registry number, VAT number, company address, and other legal metadata and terms of use have to be published as a "Site notice", "Legal notice" or "Legal disclosure". This information can be double-checked on pages like VIES/VAT number validation from the EU Commission [7] or the BBB - Better Business Bureau [8]. According to E-Commerce law, Austrian commercial companies have to have a legal notice on their webpage. In the contact section of our example website, there is no legal notice or VAT number published.

DOMAIN WHOIS

WHOIS [9] stands for "Who is?" and is a web-utility used to look up information on domain names, contact information as well as some technical information such as the domain's name servers (DNS). Every domain owner has to provide valid contact information. This is part of the registration agreement and providing false information can result in your domain name being deleted, although some types

---

[7] http://ec.europa.eu/taxation_customs/vies/
[8] http://www.bbb.org/
[9] http://www.whois.net/

of domains do allow you to have placeholder information from another company as the domain owner. By doing a whois look up on a targeted domain, you can see when a domain was registered, last updated, and how long this registration is valid. Often, scammers use the minimum period of one year to register their domain, since they are sure they will only be operating for a few months, and then they open another domain. Further important information one can gather is the hosting provider's name and contact information. This to contact the hosting provider and report the fraudulent website. It is also possible to track down inconsistencies, e.g. different addresses or website owner from what is stated on the website.

In our example the registrant contact is a Mr. Fred Bohnsack, living at 2775 Holdom Avenue in Surrey, B.C., Canada. The website is hosted with hostgator.com and is registered for one year.

REVERSE IP LOOKUP

Using a reverse IP Address lookup tool[10] it is possible to gain more insight into all the different websites and domains hosted on that IP-address. Often scammers run several websites at once, and it is just easier, cheaper and more convenient to host them under the same provider. This way, it is often possible to observe the working methods of a group of scammers who operate several websites at once.

HTML CODE AND TEXT ANALYZER

Scammers often reuse their website templates. Once their websites are taken off the Internet, they make small changes, e.g. the business

[10] `http://reverseip.domaintools.com/`

name, address, the logo or in the written text, and register a different domain and upload the site again. To be able to more quickly track down the website once it re-surfaces again, anti-scam activists use online services like 'Talkwater alerts' and 'Google alerts'. With these services one can search for certain keywords or phrases and get instant alert messages when the website is indexed. Activists specialize in certain businesses and build up alert clusters.

Another toolset that can be used to track copied content on the web are online plagiarism detection services like "citeliner" or "copyscape". Once you copy/paste phrases of the website's text into the searchbox, the services use the Google API to return websites that use the same or similar text. This way it is possible to detect websites that are clones of other websites, and with our example website we found three other fake websites and also the "real" source company, from which the content for the other websites was copied.

In addition to analyzing the text on the website, when we look into the HMTL code we find a reference that the website was "mirrored from sunexsolutions.com/ by HTTrack Website Copier/3.x [XR&CO '2013], Sat, 11 Oct 2014 06:46:46 GMT". This reveals that the website "start-office.biz" is a clone from "sunexsolutions.com". The sunexsolutions was amongst the *Megacorp.* business websites that were scraped and analyzed.

THE MEGACORP. BUSINESS CONGLOMERATE

The research of the scambaiting community "Artists against 419" led to a deeper investigation into how this community tracks fake business websites and reports them. We wanted to visualize the database, so our idea was to look at all these fake companies as though they were one big evil corporate conglomerate that wants to take over the world. This so called *Megacorp.* is inspired by

its equally powerful counterparts in science fiction. The term was coined by William Gibson and inspired many other authors of the dystopian cyberpunk science fiction genre to create megacorps in their fiction, amongst others the Tyrell corp. (*Do Androids Dream of Electric Sheep*), Encom corp. (*Tron*), Weyland-Yutani (*Alien series*), Cyberdyne Skynet Systems (*Terminator*).

The artwork is based on a collection of 1000 fake websites scraped from Internet. The creation of the *Megacorp.* serves as an umbrella company that depicts the overall business segments and countries where these fake businesses are present. An interim report was published for the exhibition, and visitors have an opportunity to browse locally through the network of fake websites. Additionally a corporate presentation video and a location reconnaissance video reflect both the imaginary and the real world outreach of the *Megacorp.*

The data gathering process took several months. From September 2014 to April 2015. The aa419-database was visited on a daily basis and websites were automatically downloaded using a site scraper tool. The scraped websites were analyzed and categorized according to business segment, street address, most prominently used color on the webpage, registered city and country.

The findings are best described in the report, yet following some key figures and reflections extracted from the CEO's Letter (*Megacorp.* Interim report: First 1000 companies):

> … We have divided our enterprise into 10 business segments, of which the biggest are 'Transport and Logistics' (32.6%), 'Banking and Finance' (21.9%) and 'Online Merchandise and Trade' (14.2%). It may come as a surprise that the 'Pet Shops and Animal Transport' (6.9%) segment has a good chance of being the fourth largest business segment. … As mentioned, our company language is

currently restricted to English, and this might limit our presence on some continents, especially Asia's lucrative market, while apparently the Chinese phishers are responsible for 85% of the domain names that were registered for phishing.

The full report and screenshots from the websites can be found on the website www.megacorp.kairus.org

KairUs is a collective of two artists, Linda Kronman (FI) and Andreas Zingerle (AT). Our work focuses on human computer and computer mediated human-human interaction with a special interest in transmedia and interactive storytelling. Since 2010 we have worked with the theme of Internet fraud and online scams, constantly shifting our focus and therefore approaching the theme from a number of perspectives, such as data security, data privacy, ethics of vigilante communities, narratives of scam e-mails, and technologies in relation to fraud.

AMRO Research Lab 2015 - servus.at

Behind the Smart World
– saving, deleting and resurfacing data
Edited by Linda Kronman and Andreas Zingerle

Published 2015 by servus.at
Kirchengasse 4
4040 Linz
AUSTRIA

ISBN: 978-3-9504200-0-5

ABOUT SERVUS

servus.at is a cultural network-based initiative in Linz, Austria. In running its own technical infrastructure, servus.at offers virtual and physical access as well as opportunities for artists and cultural producers. One of the main objectives of servus.at is to implement the ideas of a "free society" in a daily practice of cultural and artistic production dealing with technology and to develop a network of trust.

AMRO Research Blog -> research.radical-openness.org/2015

PROJECT & PROCESS MANAGEMENT: Us(c)hi Reiter

COMPILED & EDITED: Linda Kronman, Andreas Zingerle

LANGUAGE EDITING & TRANSLATION: Aileen Derieg

-> kairus.org

-> eliot.at

ACKNOWLEDGMENTS

We would like to thank the following for their contribution to this book:

De Valk Marloes
Jansen Fieke
Lakova Michaela
Samson Audrey
Selvaggio Leo
Sonntag Michael
Tiefengraber Stefan
Vavarella Emilio
Veermäe Ivar
Volkart Yvonne

We also thank the Kunstuniversität Linz, particular the Department of Time-based Media, for collaborating with us since 2008.

This publication is made possible with the fund and support from:

Bundeskanzleramt für Kunst und Kultur
Stadt Linz
Land Oberösterreich

-> kunstkultur.bka.gv.at

DESIGN/TYPESETTING/SOFTWARE:

Christoph Haag -> research.lafkon.net

This publication made it through a free software workflow based on markdown, LaTeX and the GNU Bourne-Again SHell. You are free to use, study, change, improve it under the terms of the GNU General Public License -> freeze.sh/2016/btsw

TYPEFACES:

Inconsolata by Raph Levien -> levien.com
-> fontain.org/inconsolata

HK Grotesk by Alfredo Marco Pradil -> alfredomarcopradil.com
-> fontain.org/hkgrotesk

You are free to redistribute and/or modify these fonts according to the SIL Open Font License

PAPER:

Munken Print Cream -> arcticpaper.com

PRINTED IN GERMANY -> online-druck.biz

activism, 5, 23, 44, 123, 143, 144
Agbogbloshie, 76, 121–123, 126, 128
artistic research, 8, 12, 83, 143
artlab, 12, 125, 128

cloud, 8, 10, 11, 27, 64–66, 83, 88, 112, 115, 116
cold storage, 137
consumer culture, 32, 128
control, 7, 16, 18–21, 23, 34, 42, 44, 45, 48, 57, 58, 63, 65, 88, 95, 103, 106, 115, 134, 135
crystal computing, 29

data, 7–13, 16–23, 27–30, 35–37, 42–44, 47, 53–55, 57, 58, 62, 64–67, 74, 83, 84, 86–89, 93–98, 102–117, 123–129, 133–138, 150, 151
data broker, 20
data center, 29
data industry, 20, 21, 23, 27
data privacy, 128, 129, 151
data sets, 20, 53, 54, 64
data storage, 65, 96, 125, 128
death, 10, 11, 76, 83–86
delet, 5, 7, 9–12, 20, 21, 83–88, 95, 115, 117, 123, 124, 133–136, 138
domain, 13, 109, 146–149, 151

e-waste, 7, 9, 10, 12, 66, 67, 71–74, 76, 77, 79, 121–123, 125, 128
error, 9, 43–48, 138
ethics, 12, 129, 133, 134, 144, 151

Facebook, 16, 18, 20–22, 30, 54–57, 59, 83–85, 102, 103
faces, 9, 45, 47, 53, 54, 59, 64, 73
facial recognition, 9, 47, 53, 54, 59, 104
forensics, 11, 106, 107, 111, 117, 125, 127, 128, 133, 135, 137, 138
found footage, 125
fraud, 13, 22, 43, 66, 96, 114, 121, 129, 143, 144, 149–151
Free software, 4

Ghana, 5, 12, 66, 121, 122, 127, 128
Google Inc., 9, 17, 20–22, 28–30, 42–47, 55, 83, 85, 115, 127, 146, 149

hard-drive, 5, 10–12, 65, 83, 86, 95, 96, 104, 105, 121–128, 133, 134, 136, 137

identity, 22, 30, 53–59, 83, 104, 125, 127
information technology, 31, 32
installation, 12, 45, 83, 93–98, 133–137, 144

Linz, 4, 5, 98, 117, 123
location data, 17, 19

material, 8, 11, 27, 32, 58, 63, 72, 76, 77, 86, 88, 123, 125, 127, 137
Megacorp., 13, 56, 59, 144, 149–151
memory, 46, 87, 89, 105, 126, 137

metamorphosis, 41, 42, 48
mining, 11, 65–67, 72, 74, 75, 78

National Security Agency, 124

Open Source, 4, 13, 44, 66, 124, 127, 133, 135, 143, 144
ownership, 7, 10, 12, 16, 17, 19, 35, 36, 53, 56–59, 62, 63, 65, 74, 78, 79, 83, 84, 102, 103, 107–109, 111–115, 117, 124–127, 133–135, 138, 146–148

passive reconnaissance, 143, 144
personal data, 11, 12, 18, 20, 62, 102, 106, 107, 111, 113–115
power, 7, 31, 41–44, 47, 48, 59, 88, 94, 95, 115
privacy, 7, 12, 16, 21–23, 45, 55, 65–67, 103, 108, 111, 128, 129, 151
public, 9, 17, 18, 22, 37, 45, 53, 57, 72, 83, 96, 104, 113, 117, 143
public space, 37, 53

recover, 10, 12, 75, 105, 123–128, 133–136
recycling, 5, 12, 66, 71–77, 105, 125
reflect, 9, 46, 128, 134–136, 150
resurfacing data, 7, 12, 13

save, 5, 7–9, 43, 62, 64, 65, 94, 133, 136
security, 21, 23, 28, 29, 95, 105, 109, 116, 117, 121, 129, 144, 151
server, 10, 11, 28, 37, 67, 83, 85, 93–96, 98, 103, 107, 108, 133
smart world, 5, 7, 12, 42, 73, 125, 128
smartphone, 10, 17, 22, 66, 72–74, 76, 77, 97, 116
Snowden, Edward, 67, 108, 124
social media, 18, 19, 56, 58, 62, 64, 65, 83, 84, 114
surveillance, 7, 9, 53, 54, 58, 59, 104, 107, 109

technological power, 42–44, 47, 48
third person, 8, 11, 16, 98, 102–104, 106–111, 113–115
tool, 5, 13, 18, 20–22, 33, 62, 107, 115, 124, 127, 143–146, 150
traces, 11, 19, 21, 22, 27, 29, 122, 138
tracking, 8, 9, 17, 18, 22, 62, 88, 103, 115, 116, 126, 143, 148, 149

Urme, 9, 53, 54, 58, 59

vigilante communities, 151

zombie media, 122

Creative Commons Legal Code

Attribution-ShareAlike 4.0 International

Creative Commons Corporation ("Creative Commons") is not a law firm and does not provide legal services or legal advice. Distribution of Creative Commons public licenses does not create a lawyer-client or other relationship. Creative Commons makes its licenses and related information available on an "as-is" basis. Creative Commons gives no warranties regarding its licenses, any material licensed under their terms and conditions, or any related information. Creative Commons disclaims all liability for damages resulting from their use to the fullest extent possible.

Using Creative Commons Public Licenses

Creative Commons public licenses provide a standard set of terms and conditions that creators and other rights holders may use to share original works of authorship and other material subject to copyright and certain other rights specified in the public license below. The following considerations are for informational purposes only, are not exhaustive, and do not form part of our licenses.

Considerations for licensors: Our public licenses are intended for use by those authorized to give the public permission to use material in ways otherwise restricted by copyright and certain other rights. Our licenses are irrevocable. Licensors should read and understand the terms and conditions of the license they choose before applying it. Licensors should also secure all rights necessary before applying our licenses so that the public can reuse the material as expected. Licensors should clearly mark any material not subject to the license. This includes other CC- licensed material, or material used under an exception or limitation to copyright. More considerations for licensors: `wiki.creativecommons.org/Considerations_for_licensors`

Considerations for the public: By using one of our public licenses, a licensor grants the public permission to use the licensed material under specified terms and conditions. If the licensor's permission is not necessary for any reason–for example, because of any applicable exception or limitation to copyright–then that use is not regulated by the license. Our licenses grant only permissions under copyright and certain other rights that a licensor has authority to grant. Use of the licensed material may still be restricted for other reasons, including because others have copyright or other rights in the material. A licensor may make special requests, such as asking that all changes be marked or described. Although not required by our licenses, you are encouraged to respect those requests where reasonable. More considerations for the public: `wiki.creativecommons.org/Considerations_for_licensees`

Creative Commons Attribution-ShareAlike 4.0 International Public License

By exercising the Licensed Rights (defined below), You accept and agree to be bound by the terms and conditions of this Creative Commons Attribution-ShareAlike 4.0 International Public License ("Public License"). To the extent this Public License may be interpreted as a contract, You are granted the Licensed Rights in consideration of Your acceptance of these terms and conditions, and the Licensor grants You such rights in consideration of benefits the Licensor receives from making the Licensed Material available under these terms and conditions.

Section 1 – Definitions.

a. Adapted Material means material subject to Copyright and Similar Rights that is derived from or based upon the Licensed Material and in which the Licensed Material is translated, altered, arranged, transformed, or otherwise modified in a manner requiring permission under the Copyright and Similar Rights held by the Licensor. For purposes of this Public License, where the Licensed Material is a musical work, performance, or sound recording, Adapted Material is always produced where the Licensed Material is synched in timed relation with a moving image.

b. Adapter's License means the license You apply to Your Copyright and Similar Rights in Your contributions to Adapted Material in accordance with the terms and conditions of this Public License.

c. BY-SA Compatible License means a license listed at creativecommons.org/compatiblelicenses, approved by Creative Commons as essentially the equivalent of this Public License.

d. Copyright and Similar Rights means copyright and/or similar rights closely related to copyright including, without limitation, performance, broadcast, sound recording, and Sui Generis Database Rights, without regard to how the rights are labeled or categorized. For purposes of this Public License, the rights specified in Section 2(b)(1)-(2) are not Copyright and Similar Rights.

e. Effective Technological Measures means those measures that, in the absence of proper authority, may not be circumvented under laws fulfilling obligations under Article 11 of the WIPO Copyright Treaty adopted on December 20, 1996, and/or similar international agreements.

f. Exceptions and Limitations means fair use, fair dealing, and/or any other exception or limitation to Copyright and Similar Rights that applies to Your use of the Licensed Material.

g. License Elements means the license attributes listed in the name of a Creative Commons Public License. The License Elements of this Public License are Attribution and ShareAlike.

h. Licensed Material means the artistic or literary work, database, or other material to which the Licensor applied this Public License.

i. Licensed Rights means the rights granted to You subject to the terms and conditions of this Public License, which are limited to all Copyright and Similar Rights that apply to Your use of the Licensed Material and that the Licensor has authority to license.

j. Licensor means the individual(s) or entity(ies) granting rights under this Public License.

k. Share means to provide material to the public by any means or process that requires permission under the Licensed Rights, such as reproduction, public display, public performance, distribution, dissemination, communication, or importation, and to make material available to the public including in ways that members of the public may access the material from a place and at a time individually chosen by them.

l. Sui Generis Database Rights means rights other than copyright resulting from Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, as amended and/or succeeded, as well as other essentially equivalent rights anywhere in the world.

m. You means the individual or entity exercising the Licensed Rights under this Public License. Your has a corresponding meaning.

Section 2 – Scope.

a. License grant.

1. Subject to the terms and conditions of this Public License, the Licensor hereby grants You a worldwide, royalty-free, non-sublicensable, non-exclusive, irrevocable license to exercise the Licensed Rights in the Licensed Material to:

    a. reproduce and Share the Licensed Material, in whole or in part; and

    b. produce, reproduce, and Share Adapted Material.

2. Exceptions and Limitations. For the avoidance of doubt, where Exceptions and Limitations apply to Your use, this Public License does not apply, and You do not need to comply with its terms and conditions.

3. Term. The term of this Public License is specified in Section 6(a).

4. Media and formats; technical modifications allowed. The Licensor authorizes You to exercise the Licensed Rights in all media and formats whether now known or hereafter created, and to make technical modifications necessary to do so. The Licensor waives and/or agrees not to assert any right or authority to forbid You from making technical modifications necessary to exercise the Licensed Rights, including technical modifications necessary to circumvent Effective Technological Measures. For purposes of this Public License, simply making modifications authorized by this Section 2(a) (4) never produces Adapted Material.

5. Downstream recipients.

    a. Offer from the Licensor – Licensed Material. Every recipient of the Licensed Material automatically receives an offer from the Licensor to exercise the Licensed Rights under the terms and conditions of this Public License.

    b. Additional offer from the Licensor – Adapted Material. Every recipient of Adapted Material from You automatically receives an offer from the Licensor to exercise the Licensed Rights in the Adapted Material under the conditions of the Adapter's License You apply.

    c. No downstream restrictions. You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, the Licensed Material if doing so restricts exercise of the Licensed Rights by any recipient of the Licensed Material.

6. No endorsement. Nothing in this Public License constitutes or may be construed as permission to assert or imply that You are, or that Your use of the Licensed Material is, connected with, or sponsored, endorsed, or granted official status by, the Licensor or others designated to receive attribution as provided in Section 3(a)(1)(A)(i).

b. Other rights.

1. Moral rights, such as the right of integrity, are not licensed under this Public License, nor are publicity, privacy, and/or other similar personality rights; however, to the extent possible, the Licensor waives and/or agrees not to assert any such rights held by the Licensor to the limited extent necessary to allow You to exercise the Licensed Rights, but not otherwise.

2. Patent and trademark rights are not licensed under this Public License.

3. To the extent possible, the Licensor waives any right to collect royalties from You for the exercise of the Licensed Rights, whether directly or through a collecting society under any voluntary or waivable statutory or compulsory licensing scheme. In all other cases the Licensor expressly reserves any right to collect such royalties.

Section 3 – License Conditions.

Your exercise of the Licensed Rights is expressly made subject to the following conditions.

a. Attribution.

1. If You Share the Licensed Material (including in modified form), You must:

    a. retain the following if it is supplied by the Licensor with the Licensed Material:

        i. identification of the creator(s) of the Licensed Material and any others designated to receive attribution, in any reasonable manner requested by the Licensor (including by pseudonym if designated);

        ii. a copyright notice;

        iii. a notice that refers to this Public License;

        iv. a notice that refers to the disclaimer of warranties;

        v. a URI or hyperlink to the Licensed Material to the extent reasonably practicable;

    b. indicate if You modified the Licensed Material and retain an indication of any previous modifications; and

    c. indicate the Licensed Material is licensed under this Public License, and include the text of, or the URI or hyperlink to, this Public License.

2. You may satisfy the conditions in Section 3(a)(1) in any reasonable manner based on the medium, means, and context in which You Share the Licensed Material. For example, it may be reasonable to satisfy the conditions by providing a URI or hyperlink to a resource that includes the required information.

3. If requested by the Licensor, You must remove any of the information required by Section 3(a)(1)(A) to the extent reasonably practicable.

b. ShareAlike.

In addition to the conditions in Section 3(a), if You Share Adapted Material You produce, the following conditions also apply.

1. The Adapter's License You apply must be a Creative Commons license with the same License Elements, this version or later, or a BY-SA Compatible License.

2. You must include the text of, or the URI or hyperlink to, the Adapter's License You apply. You may satisfy this condition in any reasonable manner based on the medium, means, and context in which You Share Adapted Material.

3. You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, Adapted Material that restrict exercise of the rights granted under the Adapter's License You apply.

Section 4 – Sui Generis Database Rights.

Where the Licensed Rights include Sui Generis Database Rights that apply to Your use of the Licensed Material:

a. for the avoidance of doubt, Section 2(a)(1) grants You the right to extract, reuse, reproduce, and Share all or a substantial portion of the contents of the database;

b. if You include all or a substantial portion of the database contents in a database in which You have Sui Generis Database Rights, then the database in which You have Sui Generis Database Rights (but not its individual contents) is Adapted Material, including for purposes of Section 3(b); and

c. You must comply with the conditions in Section 3(a) if You Share all or a substantial portion of the contents of the database.

For the avoidance of doubt, this Section 4 supplements and does not replace Your obligations under this Public License where the Licensed Rights include other Copyright and Similar Rights.

Section 5 – Disclaimer of Warranties and Limitation of Liability.

a. UNLESS OTHERWISE SEPARATELY UNDERTAKEN BY THE LICENSOR, TO THE EXTENT POSSIBLE, THE LICENSOR OFFERS THE LICENSED MATERIAL AS-IS AND AS-AVAILABLE, AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE LICENSED MATERIAL, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHER. THIS INCLUDES, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OR ABSENCE OF ERRORS, WHETHER OR NOT KNOWN OR DISCOVERABLE. WHERE DISCLAIMERS OF WARRANTIES ARE NOT ALLOWED IN FULL OR IN PART, THIS DISCLAIMER MAY NOT APPLY TO YOU.

b. TO THE EXTENT POSSIBLE, IN NO EVENT WILL THE LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE) OR OTHERWISE FOR ANY DIRECT, SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR OTHER LOSSES, COSTS, EXPENSES, OR DAMAGES ARISING OUT OF THIS PUBLIC LICENSE OR USE OF THE LICENSED MATERIAL, EVEN IF THE LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSSES, COSTS, EXPENSES, OR DAMAGES. WHERE A LIMITATION OF LIABILITY IS NOT ALLOWED IN FULL OR IN PART, THIS LIMITATION MAY NOT APPLY TO YOU.

c. The disclaimer of warranties and limitation of liability provided above shall be interpreted in a manner that, to the extent possible, most closely approximates an absolute disclaimer and waiver of all liability.

Section 6 – Term and Termination.

a. This Public License applies for the term of the Copyright and Similar Rights licensed here. However, if You fail to comply with this Public License, then Your rights under this Public License terminate automatically.

b. Where Your right to use the Licensed Material has terminated under Section 6(a), it reinstates:

1. automatically as of the date the violation is cured, provided it is cured within 30 days of Your discovery of the violation; or

2. upon express reinstatement by the Licensor.

For the avoidance of doubt, this Section 6(b) does not affect any right the Licensor may have to seek remedies for Your violations of this Public License.

c. For the avoidance of doubt, the Licensor may also offer the Licensed Material under separate terms or conditions or stop distributing the Licensed Material at any time; however, doing so will not terminate this Public License.

d. Sections 1, 5, 6, 7, and 8 survive termination of this Public License.

Section 7 – Other Terms and Conditions.

a. The Licensor shall not be bound by any additional or different terms or conditions communicated by You unless expressly agreed.

b. Any arrangements, understandings, or agreements regarding the Licensed Material not stated herein are separate from and independent of the terms and conditions of this Public License.

Section 8 – Interpretation.

a. For the avoidance of doubt, this Public License does not, and shall not be interpreted to, reduce, limit, restrict, or impose conditions on any use of the Licensed Material that could lawfully be made without permission under this Public License.

b. To the extent possible, if any provision of this Public License is deemed unenforceable, it shall be automatically reformed to the minimum extent necessary to make it enforceable. If the provision cannot be reformed, it shall be severed from this Public License without affecting the enforceability of the remaining terms and conditions.

c. No term or condition of this Public License will be waived and no failure to comply consented to unless expressly agreed to by the Licensor.

d. Nothing in this Public License constitutes or may be interpreted as a limitation upon, or waiver of, any privileges and immunities that apply to the Licensor or You, including from the legal processes of any jurisdiction or authority.

Creative Commons is not a party to its public licenses. Notwithstanding, Creative Commons may elect to apply one of its public licenses to material it publishes and in those instances will be considered the Licensor. The text of the Creative Commons public licenses is dedicated to the public domain under the CC0 Public Domain Dedication. Except for the limited purpose of indicating that material is shared under a Creative Commons public license or as otherwise permitted by the Creative Commons policies published at creativecommons.org/policies, Creative Commons does not authorize the use of the trademark "Creative Commons" or any other trademark or logo of Creative Commons without its prior written consent including, without limitation, in connection with any unauthorized modifications to any of its public licenses or any other arrangements, understandings, or agreements concerning use of licensed material. For the avoidance of doubt, this paragraph does not form part of the public licenses.

Creative Commons may be contacted at creativecommons.org.