dbjw
Deutsch-Baltisches
Jugendwerk

GERMAN-BALTIC CONFERENCE Tallinn 2021

“EUROPE SHALL HEAR YOU”

European Answers how to shape our Future

– POLICY PAPER –

Cluster C “Who shall own my data? Data Autonomy”

The Conference is organized by:

German-Baltic Academic Foundation. German-Baltic Youth Office

The German-Baltic Academic Foundation promotes exchange and cross-cultural understanding between young adults from Germany, the Baltic States and Russia on the basis of democracy and human rights. For this purpose, we award scholarships, organize seminars and congresses, arrange internships and facilitate networking of participants and scholarship recipients through alumni work. In the context of the shared history, the Foundation aims to continuously develop towards becoming a German-Baltic Youth Office (Deutsch-Baltisches Zukunftsforum /„DBJW“).

www.dbjw.de

This policy paper was written by:

youth ambassadors:

Andreis Gustavo Malta Purim (France, Lille)
Alexandrea Swanson (Germany, Frankfurt)
Alexander von Janowski (Germany, Munich)
Roland Markus Miitra (Estonia, Tallinn)
Amela Gjishti (Germany, Munich)

moderator:

Larissa Leiminger (Germany, Augsburg)

expert:

Helen Eenmaa (University of Tartu, Estonia, Tartu)

Table of contents

Abstract

As societies become increasingly interconnected and digital, data inherently becomes more abundant, and hence the question of “who owns my data" becomes ever more eminent. While the usage of data brings countless advantages to facilitate improved user experience and make our daily lives easier. In the same stroke, it also brings many problems, such as: personal data leaks, or profiling for political or financial gain. Currently, it is difficult to develop preventive measures to mitigate the negative effects of data usage because we as a society are not informed about how our data is being shared, used and catered to us. As a result, we need to start thinking about ways of bringing back control to individual users.

In this paper, we will explain the terms: data literacy and data transparency. Furthermore, we will point out why they are necessary for a strong European future and how these aspects lead us to the importance of an increase in data autonomy. In our last section, we will describe what a conceptual solution for increased data autonomy could look like - in the form of what we call a "data wallet". With this solution we want to demonstrate how an application that builds on data transparency and data literacy can improve an individual’s agency in accessing and controlling their shared data. Our appendix

additionally includes a first prototype concept for interested readers. Additionally, our data literacy library provides helpful links for the reader to inform themselves about this topic.

Introduction

By the time you have finished reading this sentence, nearly 200 million emails will have been sent, 69 million WhatsApp messages exchanged, and 695,000 instagram stories shared (Jenik, 2021). The pace at which data is being created, shared, and stored is incomprehensible and is changing and shaping our society more than we can pathom. To put it into perspective, over a decade ago it was estimated that every two days we created as much information as we did from the beginning of civilization to 2003 - that is around 5 billion gigabytes (Siegler, 2010). Today, in 2021, it is estimated that 2.5 quintillion bytes of data are being created daily (Johnson, 2021).

While there are many possible questions that can follow from this, one question that this policy paper will focus on is: who owns all of this data? The individuals who create it? According to the current model, the answer is: no. Up until now, the business model of some of the largest tech companies in the world is based on using individual's data for profit. Back in 2006 UK Mathematician Dr. James Bellini coined the saying, "Data is the new oil of the 21st century." And over a decade later, what he said became reality. In 2018, the Facebook-Cambridge Analytica data scandal brought mainstream light to how user data is utilized for profit. It also shed light on the topics of data security and data misuse. This scandal continues today in the form of psychological targeting via advertisement, both political and commercial by nature. What we are being shown is altering who we are, what we think, what we buy, what we believe and who we vote for. Steps in order to attenuate such data transparency issues have been taken by the European Commission in the past, for example under the General Data Protection Regulation (GDPR) of 2018. However, we argue that enough is not being done.

Hence, under the motto of the German-Batlic Conference 2021, "European Answers on how to shape our future," we want to be able to live a life free of data worries. We want to be free of advertisements which subconsciously influence who we are, what decisions we take and ultimately know the answer to the question: "who owns our data."

The purpose of this policy paper is to urge European politicians to put the topic of "who owns my data" on the top of their agendas in order to live in a society without worrying about who owns my data and what is being done with it. In order to achieve this goal, this paper will be structured in a two-step approach. First, we will explain the concept of data autonomy, comprised of its two main pillars: data literacy and data transparency. Both are important for data governance in a digital world. In contrast to data sovereignty, which is connected to statehood, data autonomy is the concept of the individual being not only capable of seeing how their data is being used and shared, but also being capable of analyzing it in a critical manner and acting to restrict or permit its usage.

In a second step, we will propose how a so-called "data wallet" could be a step towards data autonomy. In this data wallet, the user would be able to access and track- in an unified dashboard. In this dashboard, the user would be able to see where data is being shared, who is using the data and for what purposes.

Finally, our paper will conclude with how the concept of data autonomy should be discussed and practiced in the near future - be it in the political or social sphere.

Why is data autonomy important?

Why is data autonomy important to us? It is important because the way our data is being broadly exploited and monetized by big social media and analytics companies is not acceptable. We, as the European youth, wish to have a future without data worries, and we think there are many possible solutions for these problems.

Though at first sight, the digital services we use appear "free" they are not. We pay with our personal experience, which is collected in the form of the data we leave behind.

According to the "Data Monetization Market Report Scope" the market size value of data in 2020 reached USD 1.62 billion. Revenue forecast for 2027 has been estimated as USD 7.34 billion. (Grand View Research, 2020). The moments of realization, that we have been watched, and our information has been gathered for years can be quite frightening. Some tech companies might know more about us than we do ourselves. How can it be that our actions online can be predicted and for example after searching for travel blogs, to let us say France, then on the next web pages we will be confronted with ads for travel agencies offering good deals on a trip to Paris. This way of action can only be possible through data analysing algorithms and software, otherwise known as cookies.

At the same time, extreme examples like the so-called Cambridge Analytica scandal shows how our own data can be used to push us into socially undesirable directions. In the wake of the 2016 US Presidential Elections and the BREXIT referendum in Great Britain, undecided voters (referred to as persuadables) were targeted on a fine-grained basis to push them into a certain political direction. ("The Great Hack" Karim Amer, Jehane Noujaim 2019). All of this happened in a completely intransparent way, making it impossible for the individuals to know if they were targeted at all and why they were put into which kind of category.

The data collected can be used as a psychological weapon, as described by the people confessing throughout the Cambridge Analytica process. People's decisions during elections can and have been influenced by such strategies which consist of invading voters privacy, and is certainly considered to be a violation of democratic elections.

Though at first sight, the digital services we use appear "free" they are not. We pay with our personal experience, which is collected in the form of the data we leave behind.

Worrying about your personal data is cumbersome. Even with regulations in place, such as the GDPR, to allow users to access the data companies have about them - it is likely most people will not use them. Not only does the user need to personally contact every different company and ask for their data (which involves emails and a considerable amount of time), the data he will have access to will be almost unintelligible for most people - with every company giving different structures, data types and no explanation of it. This would leave only the most radical data privacists to use such regulations in their favour.

Furthermore, we are trying to avoid falling into problems such as creating new regulations, or ethical questions such as who would store this data. The objective with this solution is to make something truly applicable in real life and useful for users

Before exploring what we call "data wallet" as a potential way to regain transparency about data practices, we want to first dive deeper into the concept of "data autonomy".

How do we want to change the status quo of data autonomy?

We believe that data is something that inherently belongs to the individual that has created it. In this regard, we define data autonomy as follows: individuals (referred to as data subjects) should have the ability to understand and control their flow of data and rebuke consent if desired.

Before expanding on what we mean by data autonomy in more detail, we want to stress a few important aspects the existing General Data Protection Regulation has already achieved towards data autonomy[1]:

First, the GDPR defines the territorial scope of data processing and gives data rights to every subject in and of the European Union. This is important becasue it pins the global flow of data to European jurisdiction and provides the individual with new ways to exercise their rights in a digital world. Next, it goes on defining important terms such as "personal data", "profiling", "processing", and many more. This is important in order to create and cultivate an informed public discourse around the topic of data protection. Finally, it lays down rules for the lawful

[1] All articles are cited from the General Data Protection Regulation (Regulation (EU) 2016/679) which can be found here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

processing of personal data and most importantly, defines essential rights of data subjects. To highlight only a few, these include for example:

- Transparency to how data is collected and processed (Article 12)
- Information and access to personal data (Article 13)
- The right to be forgotten (Article 17)
- Right to data portability (Article 20)

Although this is only a small selection from the whole regulatory body, these articles are already crucial steps in an attempt to achieve data autonomy. They define obligations for the owner and processor of data and lay the basis for control of individual subjects when it comes to access, transparency and control.

We want to build upon GDPR outlined above to expand individual control into what we call data autonomy. We define data autonomy as: *the ability of the individual users to access, view and control their data either individually or in exchange with others.*

In this regard our concept of data autonomy refers to mechanisms of self-government and is built upon two main pillars: *data literacy* (1) and *data transparency* (2). Ideally, they should be considered as complementary in order for any form of regulation to achieve maximal impact.

(1) We believe that the start of any meaningful decision about the processing of one's data, data subjects need to be aware of the relevant terms. They should know what *data* is, how data *processing* works and why it is

important to care about this topic in the first place. Parts of this are already covered in the GDPR but we believe that policy makers should put a greater emphasis on making the subject in general more understandable and put greater emphasis on educating the general public. This could include cross-national courses on educating data subjects around the European Union. We see this also as a cross-generational task. With one the one side, new kids, teenagers and young adults joining data driven services. They need to be educated about how their data is used and how this affects and in some ways even manipulates them into certain undesirable directions. On the other side, we also have an increasing number of elderly people joining networks and services without any prior knowledge of data usage. Finding ways to educate the general public about these issues is a crucial pillar towards any kind of data autonomy.

Besides the definitions already included in the GDPR we would believe having clarity over the following is important to stress:

- Overview of different data types,
- Explanation of metadata and why the exact content often doesn't matter
- Cookies and why they are on every website we visit
- The meaning and relevance of *big* data
- What algorithms are and how they differ from learning systems, and
- Different types of data governance models

This list is by far exhaustive. It does, however, serve as a starting point to enlarge the discussion about data usage in our contemporary digital societies. It helps to raise awareness for how data is being used and builds the basis for any informed decision about how we want to treat data processing in the future. To further add to this, we started collecting links to important publications, podcasts, books, etc. that can be found at the end of this publication in the *Data Literacy Library* section.

(2) Although knowledge about these basic terms is necessary to make any informed decisions about data processing, in itself it is insufficient. Informed choices - whether *consent* to data collection practices in general, the *choice* of what specific service to use or ultimately *control* over one's datasets - need to be complemented with transparency about data collection practices. This brings us to our second pillar: *data transparency*

We believe that 'seeing' is an important step to 'understanding'. Thus it is decisive to have access to the particular dataset which companies are storing and for what reason they access what type of data. This is, at this point, largely unknown to the general public.

A second advantage in transparency is that requiring companies to be transparent about their data processing activities by default can incentivize companies to change their business model into less data-driven directions or at least minimize the amount of data they collect. We believe that the more transparency there is the stronger this incentive will be and that transparency will strengthen the agency of public interest to intervene in private commercial entities.

Again, GDPR has been a milestone towards data transparency. As mentioned above chapter two outlines many different rights of data subjects such as access to datasets in question (Article 12) or the right to erase existing datasets (the right to be forgotten') (Article 17). In its current form however, we believe this practice to be too spread out. Individual users have to request their data from each firm individually. This can prove to overburden the individuals which leads them to shying away from exercising this right, ultimately leaving this possibility underused.

We therefore want to take the possibilities granted in the GDPR one step further by introducing the idea of the so-called *data wallet.* The data wallet is an application that pools the information about every data subject's usage. It lists all the companies that have accessed different types of data from each respective data subject. As such the data wallet serves the purpose to not only require firms to grant access to the different types of data they have over their customers, or to afford customers a clear right of access to the data maintained by respective firms but to centralize and visualize existing data processing practices.

As such, the data wallet automates the process of getting the data, and furthermore, structuring it in a user-friendly dashboard where any "average" user could easily see how their data is being used and for what purposes. The main advantage we believe the data wallet to bring is *centralization*. Individual citizens would only have to open an application which displays the different categories of data respective companies own about them.

Centrally visualizing how one's data is being processed in an easy and understandable way is a very important step towards data transparency and thus data autonomy. At the same time, we acknowledge that this alone might not solve the problem of the overburdened data subject fully. This is why we envision the data wallet to not only visualize one's data but to also be a place for communities to form and exchange around data protection strategies. We will deepen this idea in the following section.

Overall, we believe that data autonomy is central for achieving a life without data worries. We understand data autonomy as being built on two main pillars: data literacy and data transparency. Both of them are central for achieving the overarching goal of autonomy and only in combination work together to achieve maximum impact.

To achieve this we need policy makers to emphasize the importance of literacy. We need cross-country cooperation to educate a great mass of digital users. At the same time, to achieve transparency in the form envisioned above we need stronger cross-sectoral cooperation and bring technicians, engineers and social scientists together to build something meaningful for future digital societies.

What a conceptual solution to increase data autonomy could be?

Why a Data Wallet?

As discussed previously, it is important to explore how our ideas and solutions would work in society. For that reason, we created a proposed model of a Data Wallet - one "app" which would help users regain their autonomy when managing their data and understand how it is being used

The idea of an app to help users face or manage how their data is being used is not entirely new. Since the 2017 UK elections, a group of activists called *Who Targets Me*[2] created a browser plugin to allow users to see which political parties were using ads to target them or their demographic. Currently, this plugin already has more than 50 thousand users and it is an example of how we could use technology to reach Data Autonomy.

Currently, the prototype is available on this link[3] with the source code being available here[4]. It must be noted that

[2] *https://whotargets.me/*

[3] https://andreispurim.github.io/data_wallet/

[4] https://github.com/AndreisPurim/data_wallet

the Data Wallet we propose is not the final product of our paper, but rather a tool to explain how the concept of Data Autonomy could be applied on a larger scale: not only for political elections but to all data. It is of course one of the many possible implementations of the concept and is a *mockup* prototype (not a functional app). The objective is to show how it could be used, and for politicians how they could work towards a practical solution.

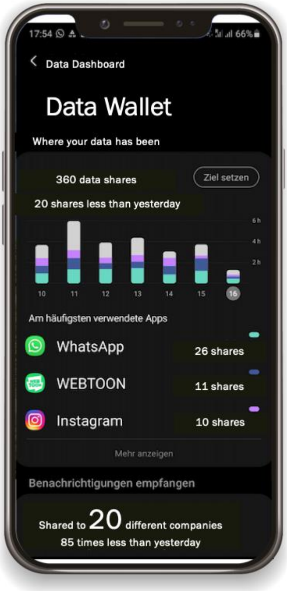
QR Code to the Data Wallet Prototype.

The Problem we are Trying to Solve

Worrying about your personal data is cumbersome. Even with regulations in place, such as the GDPR, to allow users to access the data companies have about them - it is likely most people will not use them. Not only does the user need to personally contact every different company and ask for their data (which involves emails and a considerable amount of time), the data he will have access to will be almost unintelligible for most people - with every company giving different structures, data types and no explanation of it. This would leave only the most radical data privacists to use such regulations in their favor.

Furthermore, we are trying to avoid falling into problems such as *creating* new regulations, or ethical questions such as who would store this data. The objective with this solution is to make something truly applicable in real life and useful for users

Our main inspirations - aside *Who Targets Me* - are the existing Digital Wallets and the Estonian digital ID (which serve to centralize information from multiple services, such as our Data Wallet aims to do) and the ScreenTime app, an app that allows users to see how much time they spend on each app. In our case, it would not be the time, but rather the information.



17:54 66%

Data Dashboard

Data Wallet

Where your data has been

360 data shares

Ziel setzen

20 shares less than yesterday

Am häufigsten verwendete Apps

WhatsApp	26 shares
WEBTOON	11 shares
Instagram	10 shares

Mehr anzeigen

Benachrichtigungen empfangen

Shared to 20 different companies

85 times less than yesterday

Mockup of the dashboard of the data wallet. Further information in Appendix 1.

Conclusion

The purpose of this paper is to inspire the policy makers into thinking about potential solutions of getting closer to the concept of data autonomy. The data wallet we propose gives the ordinary users full capacity to control who should own their personal data and what type of data can be shared. This way we are reaching for data transparency and literacy which are bound to be fundamental rights of the citizens in the digital world. Taking into consideration the feasibility of this solution, we would like to fully acknowledge the technical scalability complications of the Data Wallet concept. Nevertheless we strongly believe that thinking about ways to accommodate technology users in gaining full control of the data they produce in the digital environment, makes the societies we live in more democratic, intact and reputable.

Sources

Amer, K., Dreyfous, G. W., Korin, J., Kos, P. (Producers) & Noujaim, J., Amer, K. (Directors). 2019. *The Great Hack.* Retrieved from: https://www.netflix.com.

Grand View Research. 2020. Data Monetization Market Size, 2020-2027. (Report ID: GVR-4-68039-100-4) https://www.grandviewresearch.com/industry-analysis/data-monetization-market/toc#.

European Parliament. 2016. REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Jenik, Claire. 2021. Statista "A Minute on the Internet in 2021" https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet-in-one-minute/.

Johnson, Charlotte. 2021. TheNextTech. "How much Data is Produced every Day 2021?" https://www.the-next-tech.com/blockchain-technology/how-much-data-is-produced-every-day-2019/.

Siegler, MG. 2010. TechCrunch. "Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up to

2003." https://techcrunch.com/2010/08/04/schmidt-data/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKZY52ilJg0CX8CE6vX6sY9IMLAzoLLg5Cy2pKMLcqIgORtQcvaiFpY47F9zr2dmKbXKavW_sxBTYvFBXx37GEwVP2EtxCL-w-7Vd7q4-kpu7GFKRy47Xiv_5iABL_S3vcXKn-Yg39vmo_p2G_UuoUaT0t9DWVWl2YZomgzSHdA1b.

Appendix 1:

The Data Wallet: Making the Idea Reality

A more complete document of how the data app would work can be found in the source files[5], including more technical aspects of the implementation.

USAGE

First, the user would download the app on his or her phone, read the terms of service and start configuring the access to data in other apps. This step would probably take a while depending on how many other apps or services the user has. After configuring everything, the user would have access to the following tabs:

Dashboard: A ScreenTime inspired dashboard, where the user can see which apps shared or used their data in a certain time frame, and how many times each day.

Data and Logs: A dashboard where the user can see what kind of data each company/app/service has access to (this can be either sorted by company, or by type of data), and if he wants to know more, he can see a

[5] https://github.com/AndreisPurim/data_wallet

log of each usage. This “log” of each use is inspired by the Estonian ID, which signals whenever each government service uses any data from the citizen.

Currently, our prototype assumes the user would also be capable of reconfiguring the access each company has - this however requires some more technical and design capabilities which will be discussed in the technical part of the solution.

Profile and Privacy: A settings page of the app itself, where the user can opt to dissociate his other apps from the Data Wallet, re-read the terms of service, and overall uninstall the app.

Community: Another idea was to have a community tab where people concerned about their privacy or configurations could leave their comments on how to properly use or share your data, like a “forum” or a small “wikipedia”. This idea - of course - would depend on how our users interact with the app.

Technical Aspects:

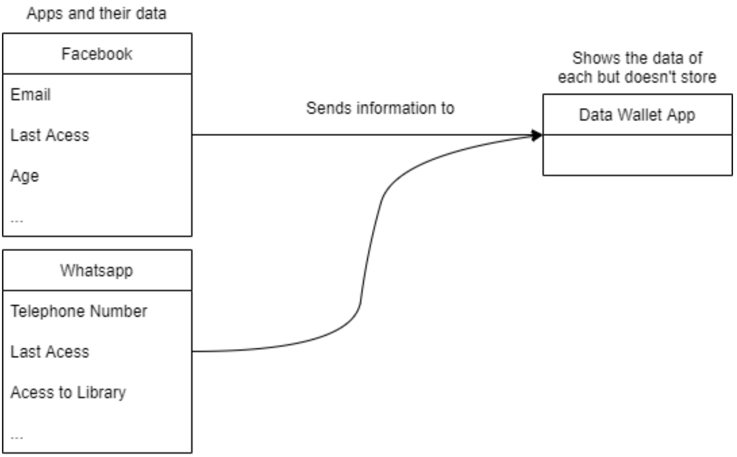
About the Current Prototype:

The current prototype is an experimental showcase of what the user would have access to and be capable of doing. It is purely a Frontend React.js-Based mockup (therefore, it is a website, not an app - and does not need to be installed), therefore, it does not have all the proposed functionalities. It is hosted in github and every person can have access to the source files and, therefore, improve or edit as they see fit. Since it was developed during the conference, it is still a very basic one.

How the data of each company would be accessed would be stored:

This question was the hardest point of contention in the development of the solution, since the app requires answers to three questions:

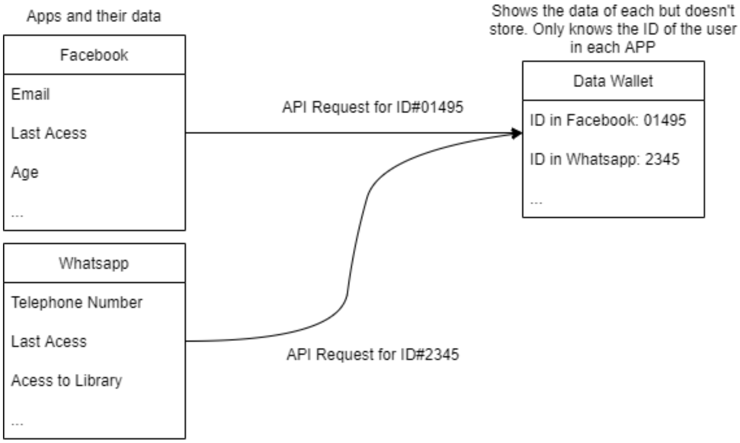
1. *Why would companies cede access to their data?* Under the GDPR, any user can request the data each company has of them. Our project would use this regulation in its favor and request the data for the app *as* the user. This would require - of course - that the user agrees for the Data Wallet to do so in the terms of service, but it would not require any additional laws.
2. *How would the app get the data of each company?* In this case, we would propose for the GDPR to standardize the access to user data through an API. Therefore, each company would have to leave an API endpoint for apps (such as the Data Wallet) to access each user data through an unique user ID. The Data Wallet app would manage the user ID of its users to each company. (see image below)



A synthethic representation of how the data is transmitted from the apps and their databases to the data wallet

3. *How would the app store the data of each company?* The answer is: it doesn't. Storing the data in the app not only would not be very useful as it would also invite technical problems (the servers necessary to store it) and legal questions (such as: is this centralization of data really safe for users?). The idea of using the API is that the app doesn't hold any information about the user other than his user ID. And every time the user opens the app, a new API call would refresh the information. Therefore, every company would still store 100% of the information of the user, and thus, there's no need to host any personal information of the user. The diagram below is a more complete diagram of the, showing how the request would "work" and highlighting that the app

DOES NOT store the data, only keeps what the ID of the user is in each app.



...

Appendix 2:

Data Literacy Library

Want to learn more about the topic of big data, data autonomy and much more? We've collected a small library of interesting books, websites, and podcasts that can help guide you on the journey.

- RadicalxChange. Website.
- James Evans: RadicalxChange(s). Podcast.
- Vi Hart (2019): Data Dignity at RadicalxChange. Article.
- Vi Hart, M Eifler (2019): Data Dignity, The Missing Market for Buying and Selling Your Data. At The Art of Research. Video.
- Center for Humane Technology. Website.
- Center for Humane Technology: Your Undivided Attention. Podcast.
- Center for Humane Technology: The Social Dilemma. Movie.
- ZDF Magazin Royal: Target Leaks. Website.
- Jaron Lanier (2018): 10 Arguments for Deleting Your Social Media Accounts Right Now. Jaron Lainer. Book.
- Jaron Lanier (2018): 10 Reasons to Get Off Social Media. On The Artificial Intelligence Channel. Video.
- Jaron Lanier (2018): How the Internet Failed and How to Recreate It. At the UC Santa Cruz Arts, Lectures and Entertainment. Video.

- Destin Sandlin (2021): Is Your Privacy An Illusion? (Taking on Big Tech) - Smarter Every Day 263. Video.
- Karim Amer, Jehane Noujaim (2019): The Great Hack. Netflix. Trailer.
- Who Targets Me. Website.
- Data for Good. Website.
- Ramesh Srinivasan (2019): Beyond the Valley. Book.
- Cathy O'Neil (2017): Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Book.
- Cathy O'Neil (2016): Weapons of Math Destruction. Talk at the Ford Foundation. Video.
- Caroline Criado Perez (2019): Invisible Women. Exposing Data Bias in a World Designed for Men. Book.
- noyb. My privacy is none of your business. Website.
- WikiLeaks. Website.
- WikiLeaks (2016): The WikiLeaks Files. The World According to US Empire. Book.
- Julian Assange (2016): Cypherpunks. Freedom and the Future of the Internet. Book.
- Edward Snowden (2019): Permanent Record. Book.
- Steven Tan & Anjaneya "Reddy" Chagam (2019): Birds of a Feather (BoF): SODA: The Path To Data Autonomy. Video.
- Soda Foundation. Website.
- Cloud Native Computing Foundation. Website.

Cluster C - Team

Andreis G. M. Purim

Andreis Purim (Andrejs Puriņš) is a Latvian-Brazilian Computer Engineer. He graduated as an Electronic Technician in the Federal University of Paraná and studies Computer Engineering (UNICAMP) in a Double Degree / Masters program at the École Centrale de Lille. He participated in Undergrad A.I. Researches (Bioinformatics, Natural Language Processing and Computer Vision).

Alexandrea Swanson

Alexandrea Swanson currently works at the American Chamber of Commerce Germany in Frankfurt in Government Relations and serves as a data protection officer. In the past she has worked to build bridges with organizations such as Fulbright and the Goethe Institute. She has a BA in International relations from Creighton University USA and a MSc in Politics, Economics and Philosophy from the

University of Hamburg. Her interest in data protection was sparked during her masters studies and while working for the German advertising company Scholz & Friends as a PR consultant. She was born and raised in Nebraska USA and has been living and working in Germany for seven years.

Alexander von Janowski

Alexander von Janowski is originally from Frankfurt where he did his undergraduate in Political Science and Economics focusing on international relations at the EU level. After finishing his bachlor he worked at the GIZ in the area of digitalisation in development cooperation. He's currently in the MSc. program Politics & Technology at the TU Munich where he focuses on questions of ethical design of technology, questions of tech governance and the future of digital democracies.

Roland Markus Miitra

Roland Miitra is an Estonian student. Currently, he is finishing his high school in the Tallinn German Gymnasium. He spent a year in Germany and finished his tenth grade there. Today he is also engaged in different projects and conferences. Afterwards he wants to study in Germany and work in different countries around the world.

Amela Gjishti

Amela Gjishti is originally from Albania. She studied computer science (cyber security) at Tennessee Tech University. She worked for two years as a Cyber Security Architect for Bank of America in Chicago, IL. Currently, she is studying Masters of Politics and Technology at the Technical University of Munich. Her passions are Ethics and Governance of Artificial Intelligence.