Position Paper: Escaping Academic Cloudification to Preserve Academic Freedom

Tobias Fiebig, Martina Lindorfer, and Seda Gürses

Privacy Studies Journal
ISSN: 2794-3941

Vol. 1, no. 1 (2022): 51-68

Introduction

The onset of the COVID-19 pandemic led to a shift in our perception of digital technologies in teaching (EdTech). While, before the pandemic, digital teaching support was a feature, a plan, or something to do in 'the future,' COVID-19 immediately turned it into a necessity. Societal use of the Internet shifted in general;[1] specific changes in academia and teaching organizations were described in the coinage of 'The Zoomification of the Classroom.[2]

As with all that is necessary, needs deemed less necessary in the situation may receive limited attention. What we, as we claim, overlooked in the Zoomification of our classrooms were the significant implications for students' and teachers' privacy rights, and the severe implications for academic freedom. Digitalization in its current form follows the established pathways of surveillance capitalism[3] and centralization[4] amassing control over what education means in the hands of a small set of major corporations.[5] We furthermore claim that the COVID-19 pandemic was not the spark that led to the Zoomification of education, but more of a catalyst, allowing necessity to push aside doubts, accelerating an ongoing process of corporate-driven centralization.

To underline our points, we revisit the results of the white paper 'Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds'.[6] As their work is of a more technical nature, we first explore what they measured, and how they obtained these results. Subsequently, we summarize their core findings and explore what these mean for the privacy, security, and digital sovereignty of students and academics around the world. Finally, we conclude with an outlook on what digital sovereignty in education should mean, and which policy steps should be taken to retain it for academic institutions.

Background

In this section, we discuss background and terms necessary for the rest of the paper. We first explore facets of privacy, most importantly, privacy as an individual right that an individual exerts control over and provides consent for, and second, privacy compliance as a mechanism used by organizations unable to provide reasonable privacy controls to

1 Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, et al., "A year in lockdown: how the waves of COVID-19 impact internet traffic," *Communications of the ACM* 64, no. 7 (Association for Computing Machinery, 2021): 101-108.

2 Mehdi Karamollahi, Carey Williamson, and Martin Arlitt, "Zoomiversity: a case study of pandemic effects on post-secondary teaching and learning," in *23rd International Conference on Passive and Active Measurement, PAM 2022. Virtual Event, March 28–30, 2022 Proceedings*, eds. Oliver Hohlfeld, Giovane Moura, and Cristel Pelsser (Cham; Springer, 2022), 573-599.

3 Nick Srnicek, *Platform Capitalism* (Hoboken: Wiley & Sons, 2017).

4 Tobias Fiebig et al. (in press). "Heads in the Clouds? Measuring Universities' Migration to Public Clouds: Implications for Privacy & Academic Freedom." *Proceedings on Privacy Enhancing Technologies Symposium* (2023).

5 Ben Williamson and Anna Hogan, "Pandemic Privatisation in Higher Education: Edtech and University Reform," *Education International* (2021).

6 Fiebig et al. "Heads in the Clouds."

individuals to still 'do' privacy. Thereafter, we discuss the history of organizational IT in higher education, and take a look at what digital sovereignty means and should mean in the context of universities.

Privacy Compliance & Individual Control

Privacy is an elusive term and comes with a myriad of facets and interpretations.[1] In work, we explore two facets of privacy: First, privacy in the context of an individual's control over their own data, i.e., their ability to make conscious decisions on who handles their data for what purpose. This essentially boils down to an individual's ability to provide informed consent for every processing of data related to themselves.[2] This notion is also what end-users commonly understand as privacy.[3]

Second, we introduce *privacy-by-compliance*, which stems from the governance reality in which we find ourselves, shaped—in Europe—by the GDPR. In a privacy-by-compliance setting an organization does not operate towards providing their users with control over their data. Instead, the major objective is putting policies and contracts in place that ensure compliance with applicable privacy legislation and policies in their corresponding jurisdiction, independently of the question whether users actually do have control over their data.

Users' control over their data may be limited by, e.g., having a technical choice to use a service, but facing real-world requirements that necessitates the use of the service. As an example, imagine a user only having one supermarket in their vicinity reachable by foot; all other supermarkets require a car. Said supermarket now introduces an external Bluetooth surveillance service for customers to improve targeted advertising, i.e., a service that tracks users' phones' Bluetooth broadcasts to identify if and how they move in a store.[4] The user is ultimately free to choose to use this supermarket and consent to the tracking, or go to any other supermarket that does not utilize such tracking. However, if the user does not have access to a car there may be socio-economic circumstances preventing them from executing their right to opt-out of data processing by using another service.

Similarly, the supermarket may claim that the use of the external service hosted in—for the sake of argument—the U.S. serves their 'legitimate interests.' Furthermore, as they may hold a contract with the processing party—under Safe Harbour or any of its decedents, i.e., the subsequent agreements put into place when the previous one was conside-

1 Helen Nissenbaum, *Privacy in Context* (Stanford: Stanford University Press, 2009).
2 Anita L. Allen, "Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm," *Conn. L. Rev.* 32 (2000): 861.
3 Kelly Caine and Rima Hanania, "Patients want granular privacy control over health information in electronic medical records," *Journal of the American Medical Informatics Association* 20, no. 1 (2013): 7-15.
4 Michael Kwet, "In Stores, Secret Surveillance Tracks Your Every Move," *The New York Times*, June 14, 2019, accessed May 30, 2022, https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

red illegal by the European Court[5]—they may claim that explicit consent from users is not even necessary, as—technically—their processing of personal data is compliant with the GDPR. Now, this argument certainly goes against common perception of privacy control, and will most likely also not hold up when scrutinized in a court of law (as Safe Harbour itself).[6] Yet, in the end it first creates an illusion of compliance, which is deemed sufficient to satisfy legal requirements, and prevents users from asking too many questions.

In this perspective, we also see how the lines between data control and data processing vanishes if privacy by compliance is employed. In fact, by creating a framework that only provides technical control to users, a data controller also enters the issue of not being able to exert control themselves. The contractual framework enables compliance but not user control, because it lacks in feasible enforcement in case of contractual violations. Hence, this lack of feasible enforcement in case of contractual violations equally applies to the data controller when a data processor only bound by privacy-by-compliance is being used; the controller has no reasonable means to enforce that a data processor does not take control of the data it is tasked to process. This may occur due to applicable laws, e.g., the Cloud Act[7] or simply due to an extensible chain of opaque sub-processors, e.g., an SaaS (Software-as-a-Service) provider ultimately using infrastructure supplied by Amazon and/or Microsoft, where the ultimate processor is not obvious, or a combination of both.

Both of these cases may seem hypothetical. Nevertheless, we revisit these points in Section 4, and see how universities fall exactly into the issues described above.

University IT: A Brief Summary

According to Fiebig et al.,[8] IT in universities clusters in three distinct pillars: teaching, research, and administration. The most common item spanning these three pillars is certainly email, which is used to communicate with students, fellow researchers, and the administration alike. In addition, each pillar has dedicated resources and requirements. For example, research infrastructure may include a graphics cards cluster for AI operations, or infrastructure for conducting online services. Teaching infrastructure usually includes a Learning Management System (LMS), which allows teachers to conduct their courses, track students' course progress, and sometimes even conduct examinations. Finally, the administration also has specific requirements, like human resource management applications, payment processing and billing systems, as well as infrastructure for handling student enrolment.[9]

5 Martin A. Weiss and Kristin Archick, *US-EU data privacy: from safe harbor to privacy shield*, Congressional Research Service, May 19, 2016.
6 Ibid.
7 Marcin Rojszczak, "CLOUD act agreements from an EU perspective," *Computer Law & Security Review* 38 (2020).
8 Fiebig et al. "Heads in the Clouds."
9 For a more comprehensive description of universities' IT infrastructure, please refer to Section II of the paper by Fiebig et al.

Digital Sovereignty in Higher Education

Digital sovereignty is one of the most commonly used terms in digital governance over the last couple of years.[10] As with all popular terms, it is rather difficult to pinpoint exactly what it means. A common interpretation revolves around nation state's ability to inflict their own governance decisions, may it be in terms of permissible content or other regulations, on digital systems under the reality of a global Internet.[11] More critical voices, such as Avila Pinto,[12] tie the matter of digital sovereignty to classical protectionism, and ultimately a form of 'digital colonialism'.

Similarly, Fiebig & Aschenbrenner[13] criticized the notion of digital sovereignty being centred around the creation of 'own' siloed systems[14] and regulatory control, [15] [16] instead of taking a perspective on the independent ability to operate, repair, and rebuild digital infrastructure.[17]

However, universities are not nation states—despite often being state organizations—especially not in the world of mostly free public education in central Europe. So, what do we mean when we talk about digital sovereignty in higher education?

Essentially, the point about digital sovereignty in higher education concerns whether digital infrastructure used by universities can negatively impact their purpose, which is usually the execution of independent research and independent teaching. This means, that external parties usually should not decide which students a university admits, what content it teaches (within certain boundaries of accreditation etc.), and what scientific research it conducts. The conglomerate of these requirements forms what is usually understood as 'academic freedom.'

Hence, when we talk about digital sovereignty being lost in higher education or academia, we are talking about a situation where the way the digital infrastructure an organization relies on is being operated puts it into a situation where its academic freedom, either in terms of research or education, may be tainted by an external party. For digital sovereignty to be lost, this external party naturally does not necessarily have to exercise

10 Julia Pohle and Thorsten Thiel, "Digital sovereignty," in *Practicing Sovereignty: Digital Involvement in Times of Crises*, ed. Bianca Herlo, Daniel Irrgang, Gesche Joost, and Andreas Unteidig (Bielefeld: transcript Verlag, 2021), 47-67.

11 Luciano Floridi, "The fight for digital sovereignty: What it is, and why it matters, especially for the EU," *Philosophy & Technology* 33, no. 3 (2020): 369-378.

12 Renata Avila Pinto, "Digital sovereignty or digital colonialism," *SUR-Int'l J. on Hum Rts*. 27 (2018): 15.

13 Tobias Fiebig and Doris Aschenbrenner, "13 propositions on an Internet for a 'burning world,'" in *Proceedings of the ACM SIGCOMM Joint Workshops on Technologies, Applications, and Uses of a Responsible Internet and Building Greener Internet* (2022).

14 Arnaud Braud et al., "The road to European digital sovereignty with Gaia-X and IDSA," *IEEE Network* 35, no. 2 (The Institute of Electrical and Electronics Engineers , 2021): 4-5.

15 Huw Roberts et al., "Safeguarding European values with digital sovereignty: An analysis of statements and policies," *Internet Policy Review* (2021).

16 Benjamin Farrand and Helena Carrapico, "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity," *European Security* 31, no. 3 (2022): 435-453.

17 Fiebig and Aschenbrenner, "13 propositions."

that opportunity; The mere chance of it being exercised is sufficient for digital sovereignty to be lost.[18]

The Pandemic Effect on Corporations and IT

The COVID19 pandemic has significantly affected all aspects of society and commerce. In terms of digital infrastructure, ranging from how we use the Internet,[19] the effect on those running and providing digital infrastructure,[20] to—as also found by Fiebig et al.—digital infrastructure in teaching and learning[21].

In addition, the pandemic also impacted global supply chains,[22] [23] while home deliveries of commodities[24] and food[25] increased, leading to considerable growth for related companies. Thus, we observe an overall growth of corporations across sectors that provided services filling the gaps in terms of consumption and social interaction, while these shifts simultaneously feed-back into human behaviour and desires.[26]

Measuring Cloudification

In this section, we provide background information on the work of Fiebig et al.[27]

Measuring Cloud Adoption

To measure universities' adoption of cloud services, Fiebig et al. utilize data from the Domain Name System (DNS). The domain name system is, essentially, like a phone book

18 See also the argument by Fiebig and Aschenbrenner on digital sovereignty being used wrong.

19 Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, et al., "The lockdown effect: Implications of the COVID-19 pandemic on internet traffic," *Proceedings of the ACM internet measurement conference* (Association for Computing Machinery, 2020): 1-18.

20 Mannat Kaur et al., "'I needed to solve their overwhelmness': How system administration work was affected by COVID-19," *25th ACM Conference on Computer-Supported Cooperative Work and Social Computing* (Association for Computing Machinery, 2022).

21 Karamollahi, Williamson, and Arlitt, "Zoomiversity."

22 Serpil Aday and Mehmet Seckin Aday, "Impact of COVID-19 on the food supply chain," *Food Quality and Safety* 4, no. 4 (2020): 167-180.

23 Remko van Hoek, "Research opportunities for a more resilient post-COVID-19 supply chain–closing the gap between research findings and industry practice," *International Journal of Operations & Production Management* 40, no. 4 (2020): 341-355.

24 Avinash Unnikrishnan and Miguel Figliozzi, "Exploratory analysis of factors affecting levels of home deliveries before, during, and post-COVID-19," *Transportation Research Interdisciplinary Perspectives* 10 (2021).

25 Diana Gavilan et al., "Innovation in online food delivery: Learnings from COVID-19." *International Journal of Gastronomy and Food Science* 24 (2021).

26 Toni D. Pikoos et al., "The Zoom effect: exploring the impact of video calling on appearance dissatisfaction and interest in aesthetic treatment during the COVID-19 pandemic," *Aesthetic Surgery Journal* 41, no. 12 (2021).

27 Fiebig et al. "Heads in the Clouds."

which allows computers to look up additional information for names. For example, when a user wants to access https://www.example.com, the DNS will be used to look up the Internet Protocol (IP) address of www.example.com, so the users' computer can establish a network connection to the server hosting www.example.com, to retrieve content from that site. Similarly, the DNS provides further functions, as for example, looking up which server is responsible for receiving emails for a specific domain, or to discover specific services related to a domain.

In their work, Fiebig et al. use a historic dataset from 2015 onwards, which essentially contains a global record of which names and associated information have been looked up by users. Please note, that this does not refer to individual users, but instead works on an aggregate of data that has been carefully processed to not include personally identifiable information.

Using this dataset, Fiebig et al. are able to investigate where sites under universities domains are hosted, whether they use a cloud-hosted learning management system, or one of the large video chat solutions (Zoom etc.), and where they receive their emails.

Core Findings

Here, for brevity, we only summarize the core findings presented by Fiebig et al.; for a comprehensive view of their results, we recommend to consult their paper. In summary, Fiebig et al.[28] find:

1. A difference between regions: According to their measurements, there is a stark contrast in cloud adoption between traditional Anglo-American influenced academic systems—the U.S., the U.K., the Netherlands, and the THE Top 100—versus continental European systems as found in Germany, France, Austria, and Switzerland. While the former group embraced the cloudification of universities' IT even before the pandemic, the latter group is more cautious, and only during the pandemic a slight uptick in adoption was measurable.

2. The impact of the pandemic on cloud adoption was focused on video lecturing: While the general cloud adoption of universities shifted into the view of public perception with the beginning of the pandemic, new adoptions were mostly clustered around video communication and collaboration tools like Zoom, WebEx, and Microsoft Teams.

3. Policy and Privacy-by-Compliance have a major impact on cloud adoption: Fiebig et al. observe that cloud adoption for email hosting was limited in the Netherlands before mid-2018. Since then, a steady uptake of, especially, Microsoft-based email hosting can be observed. As Fiebig et al. note, this coincides with a letter published by the Dutch mini-

28 Ibid.

stry of the interior, claiming that all privacy concerns regarding Microsoft's services have been resolved for Dutch government organizations.[29]

Discussion

In this section, we revisit the privacy implications of cloudification, and assess how the current cloudification measured by Fiebig et al. impacts academic freedom as a whole.

Teachers' and Students' Privacy

As outlined in Section 2.1, privacy is often understood as one's ability to freely determine who processes one's own data for what purpose. However, in a university context, this point of free decision making can be severely limited by a student's choice to pursue a certain career or field of study. If a university decides to, for example, outsource its LMS to a U.S.-based company hosting it in Amazon's EC2 cloud, it could still offer students a choice to opt out of using the LMS. However, as experience shows,[30] in these cases necessity will trump personal choice. Hence, much as in our supermarket example in Section 2.1, a student is restricted in their ability to make a free and independent choice concerning their privacy preferences. If they would prefer not to have their data processed by systems controlled by either Amazon or another U.S.-based company, their only options are to arrange themselves with this practice, or to accept that they cannot attend a course or study at a specific university.

Privacy-by-Compliance

What Fiebig et al. observe in terms of cloud service adoption is that especially those regions 'further along the path of cloudification' accumulate a multitude of services from different vendors (even though most of them ultimately rely on one of the big providers of cloud infrastructure, i.e., Google, Amazon, and Microsoft). This makes it increasingly difficult for universities to offer its users—may it be students, researchers, or teachers—fine-grained control over where their data is processed and how. At the same time, especially European institutions, find themselves struggling with the implementation of data protection legislation.[31] This may create an environment in which universities prioritize technical compliance with regulations over that actual control. Common methods to create this 'privacy-by-compliance' include, for example, unspecific and broad privacy policies essentially covering any conceivable cloud service, while using contractual agre-

29 Ferd Grapperhaus and Kajsa Ollongren, "Verificatie op de uitvoering van het overeengekomen verbeterplan met Microsoft", accessed May 30, 2022, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail? id=2019Z13829&did=2019D28465.

30 Bart Custers, Simone van der Hof, and Bart Schermer, "Privacy expectations of social media users: The role of informed consent in privacy policies," *Policy & Internet* 6, no. 3 (2014): 268-295.

31 Vincenzo Mangini, Irina Tal, and Arghir-Nicolae Moldovan, "An empirical study on the impact of GDPR and right to be forgotten-organisations and users perspective," in *Proceedings of the 15th International Conference on Availability, Reliability and Security* (2020), 1-9.

ements with suppliers to outsource responsibility for data protection aspects. To further explore this subject, we recommend the reader to take a look at their own institution's privacy policy—if they can find it.

As the main tool of privacy-by-compliance, Universities' privacy policies are an ideal place to investigate the prevalence of privacy-by-compliance.[32] Coghlan et al.[33] studied the privacy policies of 23 popular EdTech tools and found that universities often negotiate their own terms and conditions, which also impacts data processing. Thus, instead of focusing on the privacy policies of individual platforms, we also studied the publicly available privacy policies of each country's top-three universities (THE Top100, 21 universities, 46 documents) to identify how they communicate their cloud use. We find two types of documents: (1) privacy policies describing data collection/processing activities, and (2) data protection guidance (not publicly available for 4 universities).[34]

The public-facing documents we surveyed are exclusively focused on data controller and FERPA responsibilities,[35] i.e., data and student records collected and processed by the universities using their own IT infrastructure. German universities stood out with policies being detailed and emphasizing subject access rights. Still, despite the high cloud-usage found by Fiebig et al.,[36] we did not find one university that provides a comprehensive overview of what data is collected by and shared with these infrastructures. Instead, the data shared is summarized in broad terms like "platform usage and interaction data", and is regularly hidden in auxiliary documents. While third-party cloud services used in websites, e.g., social media buttons, are mentioned regularly, references to third-party services used in university administration and operations were scarce. Some universities noted contractual agreements with third-party cloud providers to limit purpose of data collection and processing, but not a single one provided further details on the implementation of these contracts. Hence, in summary, universities seem to approach the issue of a growing set of cloud dependencies by applying privacy-by-compliance.

Another aspect in this framework is the role of the student in this setup. As Fiebig et al. note, a progressing cloudification may intersect with a further developed self-understanding as an economic entity of an academic institution, or rather, the encouragement of such positions by an academic system at large. The continuous influx of traditional management methods into academia—progress reports, Key Performance Indicators

32 Simon Coghlan, Tim Miller, and Jeannie Paterson, "'Good proctor' or 'Big Brother'? AI Ethics and Online Exam Supervision Technologies," *Philosophy & Technology* (2021).

33 Ibid.

34 All documents we analysed are available online: https://github.com/headsinthecloud/universities.

35 U.S. Department of Education "Family Educational Rights and Privacy Act (FERPA)", accessed November 11, 2022, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

36 Fiebig et al., "Heads in the Clouds."

(KPIs), and a drive to 'valorize'[37] research, sometimes even included as a KPI—has been ongoing for several years, and has equally been criticized[38] and applauded.[39]

A necessary corner stone in the use of privacy-by-compliance is, however, the acceptance of users as a form of employee, i.e., as people hired or integrated into the organization for a purpose and use.[40] This transforms their privacy concerns in the work environment from a private matter of their own to a simple question of organizational compliance, in which the organization can make decisions for them, as it is essentially just a decision for itself. There are arguments to be had on whether this perspective is valid—even for employees[41]—yet such a stance simplifies the process of creating privacy-by-compliance. Systems are there for a purpose; if usage is restricted to business relevant activities only, there is far fewer private data to be handled.

We, the authors, obviously disagree with this perspective, especially in the context of universities and education. We argue that taking such a perspective of privacy-by-compliance, which includes the necessary leap of interpreting students as a form of employees of the university system, fundamentally conflicts with the idea of an academic environment enabling students to execute (and attain the ability to execute) free and independent thoughts.[42] We would, in fact, go as far as claiming that education itself is one of the most private matters in our society. The ability to develop ideas is rooted in an ability to be wrong. Recording our learning progress—detailed and fine-grained—might make our learning errors a permanent record in cloud infrastructure outside of our control, or at least carries the threat of them becoming a permanent record. In turn, this ominous threat might inhibit the learning progress of students: Cautious to not create a permanent record of them challenging the status quo or being out-of-their-depth when exploring new fields and subjects, they may move towards safe and predictable options. In that sense, the effect is similar to how a threat of privacy violations and surveillance leads to a change in attitude, as people align their behavior with the expectation of being observed.[43]

Hence, in summary, we claim that if an academic organization attempts to implement privacy-by-compliance instead of leaving its students (and to a degree teachers) with the ability to control the spread of their data, it ultimately fails its own purpose.

37 Here, valorization, verb 'to valorize', refers to the process of successfully disseminating and promoting research results, especially converting research results into a tangible and monetary benefit for the organization, for example, by obtaining and selling patents, or by creating a start-up company rooted in research results.

38 Deborah Churchman, "Voices of the academy: academics' responses to the corporatizing of academia," *Critical Perspectives on Accounting* 13, no. 5-6 (2002): 643-656.

39 Adrienne S. Chan and Donald Fisher, eds., *The Exchange University: Corporatization of Academic Culture* (Vancouver: UBC Press, 2009).

40 Sara Ahmed, *What's the use?: On the uses of use* (Durham, NC: Duke University Press, 2019).

41 Lothar Determann and Robert Sprague, "Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States," *Berkeley Tech. LJ* 26 (2011): 979.

42 Ahmed, *What's the use?* See also the humboldtian ideal of education.

43 Nina Gerber, Paul Gerber, and Melanie Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & Security* 77 (2018): 226-261.

Academic Freedom

In Section 2.3, we briefly discussed the meaning of digital sovereignty in the context of higher education. We now shift this discussion into the context of academic freedom. Fiebig et al.[44] claim, that the progressing cloudification of universities' IT may ultimately threaten academic freedom. However, the underlying mechanics of how this comes to be, as well as the historic embedding, remains—to a degree—unclear in their work.

As with the issue with privacy-by-compliance, this boils down to the ultimate purpose of academia as a cradle of independent thought. Even though we acknowledge that this ideal is often betrayed by academics themselves, we use it as an assumption in our argument, making our claims within the framework of an ideal world.

A glowing and well-documented example of the corrective power of academia—and the corporate need to spend excessive resources on preventing truth to be acknowledge by society—is certainly the issue of lead pollution.[45] Patterson, the first scientist to establish the age of the earth, also noticed that there was an apparent human-made poisoning of the environment by the then commonly leaded gasoline.[46] Facing this discovery, especially oil and gas corporations expended significant resources to discredit Patterson and prevent his results from appearing, allegedly going as far as promising him nearly unlimited third-party funding if he would only vow to not pursue this line of research.[47]

Now, what enabled Patterson to continue his work was (a) academic freedom, and (b) his adversaries lacking a direct measure of exerting pressure. More boldly speaking, while oil and gas companies could try to buy him, and could fund research 'disproving' his findings ad infimum, there was no lever to take something from him or his institution.

Cloudification and questionable funding resemble one another in that they challenge/threaten scientific independence.[48] As Fiebig et al.[49] claim, there is, however, an inherent difference in the fact that cloudification gives corporations who operate in the heart of academia a direct lever to influence the academic discourse on the negative impact of said corporations.[50] They may, for example, put pressure on a university whose researchers conduct work that is perceived by the corporation as a threat to itself.

44 Fiebig et al. "Heads in the Clouds."

45 We note that we could also use the human-made climate crisis currently ravaging our world as an example here. However, for that incident sadly no common consensus on how bad the situation is has been reached yet, even though several corporations have been caught—knowing how bad the state of climate change is—trying to discredit climate researchers in order to sway public opinion their way. Similar effects have also been observed around the tobacco industry.

46 Clair C. Patterson, "Contaminated and natural lead environments of man," *Archives of Environmental Health: An International Journal* 11, no. 3 (1965): 344-360.

47 Neil Degrasse-Tyson, "The Clean Room," *Cosmos: A Spacetime Odyssey*. Fox Broadcasting, April 20, 2014.

48 Sylvia Rowe, Nick Alexander, Fergus Clydesdale, Rhona Applebaum, Stephanie Atkinson, Richard Black, Johanna Dwyer et al., "Funding food science and nutrition research: financial conflicts and scientific integrity," *Nutrition Reviews* 67, no. 5 (2009): 264-272.

49 Fiebig et al. "Heads in the Clouds."

50 Shoshana Zuboff, "Big other: surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology* 30, no. 1 (2015): 75-89.

Imagine, for example, a university migrating their email infrastructure to Google. At the moment, according to Fiebig et al., this concerns at least 10% of all U.S. R1/R2 universities. Then, let's say, that university conducts research that is not in the best interest of Google. They may find that the contributions of Google to the field of machine learning are not benefiting society,[51] they might talk about how large language models are severely biased and thus introducing harms to society,[52] or they may simply find Google to execute unfair business practices.[53] While, traditionally, Google would be able to exert pressure only by, e.g., reducing third-party funding to this institution, they now have a very direct lever. No law forces one organization to conduct business with another. In a free market, even infrastructure-providers—and there are many—are free to decide with whom they want (and do not want) to work. Technically, Google could decide to discontinue the business relationship regarding a cloud-hosted email solution with the university. While, of course, the university could always start hosting their own systems again, this comes with significant knowledge requirements,[54] most certainly knowledge migrated out of the institution as part of the cost-saving measures of outsourcing in the first place.[55] Furthermore, an email migration—even to another vendor—always incurs significant costs and disruption of services, no matter how well it is executed. Of course, this additional cost differs between the type of service being used, and ties closely to the amount of data stored along with it. For example, a comparatively complex service may be cheaper to migrate than a simple service relying on petabytes of data. At the same time, for specific services the number of reasonable choices may be limited. When it comes to enterprise-scale email, for example, choices are essentially limited to products from Google and Microsoft. Similarly, the number of providers of Learning Management Systems is limited, and—at the time of writing—all of these ultimately use Amazon's cloud infrastructure to provide their services.

Hence, all of the sudden, Google could do something inflicting direct harm to punish an institution, without even doing something illegal.[56] The notion of this being sudden might sound surprising here. After all, contractual agreements should have terms and conditions that prevent their sudden termination. However, especially in business-to-business interactions, these terms can turn out to be surprisingly short. Furthermore, quiet recently, Google actually used the issue of urgency to renegotiate contractual terms with several

51 Reddit, accessed May 30, 2022, https://www.reddit.com/r/MachineLearning/comments/uyratt/d_i_dont_really_trust_papers_out_of_top_labs/.

52 Emily M. Bender, Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell, "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery, 2021), 610-623.

53 Brian William Jones, "The unlimited storage that Google promised my university is being discontinued," Twitter, accessed May 30, 2022, https://web.archive.org/web/20221129194157/https://twitter.com/bwjones/status/1490802506628145153.

54 Florian Holzbauer, et al., "Not that Simple: Email Delivery in the 21st Century," *USENIX Annual Technical Conference* (2022).

55 Monica Belcourt, "Outsourcing—The benefits and the risks," *Human resource management review* 16, no. 2 (2006): 269-279.

56 Please note, at this point, that Google is just a place holder for any hypergiant providing services a university may become dependent upon. The same argument stands for Microsoft, Oracle, Amazon, Zoom, Facebook, Apple, and many more, some of which have already been caught in actions similar to those described here.

major U.S. universities: After the universities had used the file storage that Google had initially offered them unlimited and free, for petabytes of data, Google abruptly provided them with for petabytes of data, Google quickly urged them to renegotiate the terms for a significantly higher price.[57][58] Furthermore, such considerations leave the power dynamics and especially power imbalance in terms of legal capabilities and funds out of scope. In business-to-business activity, the least desirable result in case of a breach of contract is a lengthy lawsuit. This then has the potential of leading to—ultimately—reasonable restitution payment. However, in contrast to the potential gain of influence on a research agenda such a restitution payment is negligible for major corporations. Furthermore, in comparison to the resources and stamina of hypergiants'[59] legal departments, universities' ability to defend themselves is, most likely, limited.

It is also important to note that these interactions, occurred before—although not on a major scale. Zoom intervened in a seminar that was not aligned with their corporate values,[60] Facebook terminated researchers' private Facebook accounts,[61] and Google reportedly used an organization's dependence as a sales mechanic.[62] Similarly, we have seen how corporations with similar financial resources tried and keep trying to increase climate disaster denial and discredit climate science for their own benefit.[63]

Ultimately, no matter how one stands on whether large cloud corporations would use their market power to further their own gains—and we argue that as rational actors they can be expected to do so—for academic sovereignty and freedom as outlined in Section 2.3, the mere chance they could is already the worst-case scenario.

Controversial Content and Centralization

The aforementioned power of hypergiants extends beyond the academic context. As Fiebig and Aschenbrenner note in their '13 Propositions on an Internet for a Burning World', the prevalence and commoditization of large-scale denial of service attacks created a situation where independent or self-hosting of content on the Internet has become challenging. Thus, it is difficult for smaller agents to publish content on the Internet without resorting to use the infrastructure of major cloud providers, may it be Amazon, Akamai, or Cloudflare. Hence, refusal of major cloud providers to 'protect' a site hosting speech they do not agree with may effectively limits an entities' ability to share said speech. This means that a majority of hate and misinformation sites are hosted on major providers, as

57 Slashdot N.D.a, accessed November 11, 2022, https://hardware.slashdot.org/story/22/02/14/1433256/.

58 Slashdot N.D.b, accessed November 11, 2022, https://tech.slashdot.org/story/22/10/03/2327248/universities-adapt-to-googles-new-storage-fees-or-migrate-away-entirely.

59 'Hypergiants' is a term from the scientific field of network measurement. The term encompasses large multi-national cloud and technology corporations like, for example, Amazon, Google, or Facebook.

60 NYU-AAUP Executive Committee, "Statement from the NYU-AAUP on Zoom Censorship Today," accessed May 30, 2022, https://academeblog.org/2020/10/23/statement-from-the-nyu-aaup-on-zoom-censorship-today/.

61 Barbara Ortutay, "Facebook shuts out NYU academics' research on political ads," accessed May 30, 2022, https://apnews.com/article/technology-business-5d3021ed9f193bf249c3af158b128d18.

62 Jones, "The unlimited storage."

63 Shannon Hall, "Exxon knew about climate change almost 40 years ago," *Scientific American* 26 (2015).

for example, Cloudflare.[64] As of recently, there was a discussion on whether Cloudflare should stop providing services to Kiwi Farms, a site conducting targeted harassment that has been linked to at least three suicides.[65]

Conclusion and Recommendations

In this paper, we took a perspective on the findings of Fiebig et al. on the cloudification of universities. We reiterated and expanded their arguments and further illuminated the connection between privacy, the ability to control one's own data, education, and academic freedom. In addition, we elaborated upon the argument of corporations using positions of power to align researchers with their own interests, sourcing from historic examples. The major remaining question is: What can we, what can academia, what can society, do to counteract these effects?

Fiebig et al. provided commonplace answers.[66] They proclaim that universities should organize and collaborate to build research and teaching infrastructure that is controlled in a democratic and transparent manner by public institutions. While this argument holds true in a tautological manner, it is also fairly naïve: The cloudification of universities is driven by socio-economic circumstances and a desire of scale and growth. However, as in other contexts, we might have to realize that eternal growth is not sustainable.[67] Instead of following the idea that digitalization enables more; more growth, more revenue, more profit, more students, more research, more everything. The fundamental question we have to ask ourselves is whether privacy and academic freedom in higher education should become a matter of sustainable infrastructures. Hence, in addition to Fiebig et al.'s recommendations, we demand not only public infrastructures for public services, but instead sustainable infrastructures. We claim that, when truly sustainable, the question of privacy and academic freedom will solve themselves.

64 Catherine Han, Deepak Kumar, and Zakir Durumeric, "On the Infrastructure Providers That Support Misinformation Websites," *Proceedings of the International AAAI Conference on Web and Social Media* 16 (2022).

65 Joseph Menn and Talor Lorenz, "Under pressure, security firm Cloudflare drops Kiwi Farms website", *Washington Post*, September 3, 2022, accessed November 11, 2022, https://www.washingtonpost.com/technology/2022/09/03/cloudflare-drops-kiwifarms. Please note that the authors are strongly convinced that this specific example, KiwiFarms, is a harmful entity that was only allowed to remain connected to the rest of the Internet due to carefully exploiting a claim of free speech to hide their illegal activity, i.e., by reframing targeted harassment as a matter of speech. Hence, while we ultimately agree with Cloudflare's decision to terminate services for the site, and note the harm done by Cloudflare's hesitation towards reaching this conclusion, we also note the challenge for society created by a private company being in a position to make that decision.

66 Fiebig et al., "Heads in the Clouds."

67 Donella H. Meadows, Dennis L. Meadows, Jørgen Randers, and William W. Behrens, "The limits to growth," in *Green Planet Blues*, eds. Ken Conca and Geoffrey Dabelko (London: Routledge, 2018), 25-29.

Disclosure Statement

None of the authors have conflicts of interest regarding the subject matter of this work, apart from being academics, working in the system we describe.

Acknowledgements

Our work was enabled by the use of a self-hosted Nextcloud instance, Signal (hosted on Amazon EC2), Google Scholar, Microsoft Office, and a self-hosted BigBlueButton instance. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of their host institutions.

Bibliography

Aday, Serpil, and Mehmet Seckin Aday. "Impact of COVID-19 on the food supply chain." *Food Quality and Safety* 4.4 (2020): 167-180.

Ahmed, Sara. *What's the use?: On the uses of use.* Durham, NC: Duke University Press, 2019.

Allen, Anita L. "Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm." *Conn. L. Rev*. 32 (2000): 861.

Avila Pinto, Renata. "Digital sovereignty or digital colonialsim." *SUR-Int'l J. on Hum Rts*. 27 (2018): 15.

Belcourt, Monica. "Outsourcing—The benefits and the risks." *Human resource management review* 16, no. 2 (2006): 269-279.

Bender, Emily M., Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?." In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery, 2021): 610-623.

Braud, Arnaud, et al. "The road to European digital sovereignty with Gaia-X and IDSA." *IEEE Network* 35, no. 2 (The Institute of Electrical and Electronics Engineers, 2021): 4-5.

Caine, Kelly, and Rima Hanania. "Patients want granular privacy control over health information in electronic medical records." *Journal of the American Medical Informatics Association* 20, no. 1 (2013): 7-15.

Chan, Adrienne S., and Donald Fisher, eds. *The exchange university: Corporatization of academic culture*. Vancouver: UBC Press, 2009.

Churchman, Deborah. "Voices of the academy: academics' responses to the corporatizing of academia." *Critical Perspectives on Accounting* 13, no. 5-6 (2002): 643-656.

Coghlan, S., T. Miller, and J. Paterson. "Good proctor or "Big Brother"? AI Ethics and Online Exam Supervision Technologies." *Philosophy & Technology* (2021).

Custers, Bart, Simone van der Hof, and Bart Schermer. "Privacy expectations of social media users: The role of informed consent in privacy policies." *Policy & Internet* 6, no. 3 (2014): 268-295.

Degrasse-Tyson, Neil. "The Clean Room." *Cosmos: A Spacetime Odyssey*. National Geographic, Fox Broadcasting, April 20, 2014.

Determann, Lothar, and Robert Sprague. "Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States." *Berkeley Tech. LJ* 26 (2011): 979.

Farrand, Benjamin, and Helena Carrapico. "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity." *European Security* 31, no. 3 (2022): 435-453.

Feldmann, Anja, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, et al. "The lockdown effect: Implications of the COVID-19 pandemic on internet traffic." *Proceedings of the ACM internet measurement conference* (Association for Computing Machinery, 2020): 1-18.

Feldmann, Anja, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, et al. "A year in lockdown: how the waves of COVID-19 impact internet traffic." *Communications of the ACM* 64, no. 7 (Association for Computing Machinery, 2021): 101-108.

Fiebig, Tobias, Seda Gürses, Carlos H. Gañán, Erna Kotkamp, Fernando Kuipers, Martina Lindorfer, Menghua Prisse, and Taritha Sari. "Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds." *arXiv preprint arXiv*:2104.09462 (2021).

Fiebig, Tobias, and Doris Aschenbrenner. "13 propositions on an Internet for a 'burning world'." *Proceedings of the ACM SIGCOMM Joint Workshops on Technologies, Applications, and Uses of a Responsible Internet and Building Greener Internet* (2022).

Floridi, Luciano. "The fight for digital sovereignty: What it is, and why it matters, especially for the EU." *Philosophy & Technology* 33, no. 3 (2020): 369-378.

Gavilan, Diana, Adela Balderas-Cejudo, Susana Fernández-Lores, and Gema Martinez-Navarro. "Innovation in online food delivery: Learnings from COVID-19." *International Journal of Gastronomy and Food Science* 24 (2021): 100330.

Gerber, Nina, Paul Gerber, and Melanie Volkamer. "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior." *Computers & Security* 77 (2018): 226-261.

Grapperhaus, Ferd, and Kajsa Ollongren. *Verificatie op de uitvoering van het overeengekomen verbeterplan met Microsoft*. 2019. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail? id=2019Z13829&did=2019D28465 accessed May 30, 2022.

Hall, Shannon. "Exxon knew about climate change almost 40 years ago." *Scientific American* 26 (2015).

Han, Catherine, Deepak Kumar, and Zakir Durumeric. "On the Infrastructure Pro-

viders That Support Misinformation Websites." *Proceedings of the International AAAI Conference on Web and Social Media* 16 (Association for the Advancement of Artificial Intelligence, 2022).

van Hoek, Remko. "Research opportunities for a more resilient post-COVID-19 supply chain–closing the gap between research findings and industry practice." *International Journal of Operations & Production Management* 40, no. 4 (2020): 341-355.

Holzbauer, Florian et al., "Not that Simple: Email Delivery in the 21st Century." *USENIX Annual Technical Conference* (2022).

Jones, Brian William . "The unlimited storage that Google promised my university is being discontinued", Twitter, URL: https://web.archive.org/web/20221129194157/https://twitter.com/bwjones/status/1490802506628145153, accessed May 30, 2022.

Karamollahi, Mehdi, Carey Williamson, and Martin Arlitt. "Zoomiversity: a case study of pandemic effects on post-secondary teaching and learning." *International Conference on Passive and Active Network Measurement.* Cham: Springer, 2022: 573-599.

Kaur, Mannat, Simon Parkin, Marijn Janssen, and Tobias Fiebig. "'I needed to solve their overwhelmness': How system administration work was affected by COVID-19." *25th ACM Conference on Computer-Supported Cooperative Work and Social Computing* (Association for Computing Machinery, 2022).

Kwet, Michael, "In Stores, Secret Surveillance Tracks Your Every Move," The New York Times, June 14, 2019, https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html, accessed May 30, 2022.

Mangini, Vincenzo, Irina Tal, and Arghir-Nicolae Moldovan. "An empirical study on the impact of GDPR and right to be forgotten-organisations and users perspective." *Proceedings of the 15th International Conference on Availability, Reliability and Security* (2020):1-9.

Meadows, Donella H., Dennis L. Meadows, Jørgen Randers, and William W. Behrens. "The limits to growth." In *Green Planet Blues: Critical Perspectives on Global Environmental Politics*, edited by Ken Conca and Geoffrey Dabelko, 25-29. Abingdon: Routledge, 2018.

Menn, Joseph, and Talor Lorenz. "Under pressure, security firm Cloudflare drops Kiwi Farms website," *Washington Post*, September 3, 2022, https://www.washingtonpost.com/technology/2022/09/03/cloudflare-drops-kiwifarms/, accessed November 11, 2022.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2009.

NYU-AAUP Executive Committee. "Statement from the NYU-AAUP on Zoom Censorship Today." Academe Blog, October 23, 2020. https://academeblog.org/2020/10/23/statement-from-the-nyu-aaup-on-zoom-censorship-today/, accessed May 30, 2022.

Ortutay, Barbara. "Facebook shuts out NYU academics' research on political ads",

AP News, August 5, 2021, https://apnews.com/article/technology-business-5d3021ed9f193bf249c3af158b128d18, accessed May 30, 2022.

Patterson, Clair C. "Contaminated and natural lead environments of man." *Archives of Environmental Health: An International Journal* 11, no. 3 (1965): 344-360.

Pikoos, Toni D., Simone Buzwell, Gemma Sharp, and Susan L. Russell. "The Zoom effect: exploring the impact of video calling on appearance dissatisfaction and interest in aesthetic treatment during the COVID-19 pandemic." *Aesthetic Surgery Journal* 41, no. 12 (2021): NP2066-NP2075.

Pohle, Julia, and Thorsten Thiel. "Digital sovereignty." In *Practicing Sovereignty: Digital Involvement in Times of Crises*, eds. Bianca Herlo, Daniel Irrgang, Gesche Joost, and Andreas Unteidig, 47-67. Bielefeld: transcript Verlag, 2021.

Reddit, https://www.reddit.com/r/MachineLearning/comments/uyratt/d_i_dont_really_trust_papers_out_of_top_labs/, accessed May 30, 2022.

Roberts, Huw, Josh Cowls, Federico Casolari, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi. "Safeguarding European values with digital sovereignty: An analysis of statements and policies." *Internet Policy Review* (2021).

Rojszczak, Marcin. "CLOUD act agreements from an EU perspective." Computer Law & Security Review 38 (2020): 105442.

Rowe, Sylvia, Nick Alexander, Fergus Clydesdale, Rhona Applebaum, Stephanie Atkinson, Richard Black, Johanna Dwyer, et al. "Funding food science and nutrition research: financial conflicts and scientific integrity." *Nutrition Reviews* 67, no. 5 (2009): 264-272.

Slashdot, N.D.a https://hardware.slashdot.org/story/22/02/14/1433256/, accessed November 11, 2022.

Slashdot N.D.b https://tech.slashdot.org/story/22/10/03/2327248/universities-adapt-to-googles-new-storage-fees-or-migrate-away-entirely, accessed November 11, 2022.

Srnicek, Nick. *Platform Capitalism*. Hoboken: Wiley & Sons, 2017.

U.S. Department of Education. Family Educational Rights and Privacy Act (FERPA). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html, accessed November 11, 2022.

Unnikrishnan, Avinash, and Miguel Figliozzi. "Exploratory analysis of factors affecting levels of home deliveries before, during, and post-COVID-19." *Transportation Research Interdisciplinary Perspectives* 10 (2021): 100402.

Weiss, Martin A., and Kristin Archick. "US-EU data privacy: from safe harbor to privacy shield." *Congressional Research Service* May 19, 2016.

Williamson, Ben, and Anna Hogan. "Pandemic Privatisation in Higher Education: Edtech and University Reform." *Education International* (2021).

Zuboff, Shoshana. "Big other: surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30, no. 1 (2015): 75-89.