Selected Papers of #AoIR2024:
The 25th Annual Conference of the
Association of Internet Researchers
Sheffield, UK / 30 Oct - 2 Nov 2024

THE 'GOOGLISATION' OF THE CLASSROOM: HOW DOES THE PROTECTION OF CHILDREN'S PERSONAL DATA FARE?

Kruakae Pothong
London School of Economics and Political Science

Louise Hooper
Garden Court Chambers

Sonia Livingstone
London School of Economics and Political Science

Ayça Atabey
University of Edinburgh

Emma Day
Techlegality

Google In The Classroom

The COVID-19 pandemic accelerated the adoption and use of diverse technologies for education (EdTech) to deliver remote learning. Google Classroom, a core service within Google Workspace for Education, is among these EdTech products that made their way into children's classrooms and have remained there since. While EdTech products like Google Classroom can benefit teachers in assigning and tracking homework submissions and facilitating remote learning (DfE, 2021a), they may expose children to data protection risks with unknown consequences for children and their life prospects (Livingstone et al., 2024).

Vast venture capital is invested in EdTech worldwide (Davies et al., 2022), with a handful of major platforms dominating the education landscape, recontextualising once-public institutions of learning within the corporate sphere (Cobo & Rivas, 2023). Given the prevalence of Google Classroom, downloaded 1.34 million times in the UK in 2021 (Clark, 2022) and endorsed by the Department for Education (DfE, 2021b), this paper examines the use of Google's compliance with data protection laws. Critical analysis of

Suggested Citation (APA): Pothong, K., Hooper, L., Livingstone, S., Atabey, A., & Day, E. (2024, October). The '*Googlisation' of the Classroom: How Does the Protection of Children's Personal Data Fare?*. Paper presented at AoIR2024: The 25th Annual Conference of the Association of Internet Researchers. Sheffield, UK: AoIR. Retrieved from http://spir.aoir.org.

digital services, such as Google Classroom, is variously theorised, including in relation to the Googlisation of education (Kerssens & van Dijck, 2021; Vaidhyanathan, 2012), although detailed analysis of EdTech's data protection practices is only recently gaining attention (West, 2023).

Our methods combine legal analysis of the privacy policies of Google Classroom and related services with a socio-technical investigation of Google Classroom's user journey with a small number of children. We deployed Lightbeam (for Firefox) and Thunderbeam (for Chrome) to capture the data flow throughout each child's user journey. Our aim was to investigate the platform's operation given the applicable policies and data protection regulations rather than sampling families representatively.

This research was funded by the 5Rights Foundation and approved by the Ethics Committee of the London School of Economics and Political Science (LSE) as part of the Digital Futures for Children's work.

What Is The Problem With Google Classroom?

Legal analysis of the privacy policies governing Google Classroom and other Google services accessible to children in the Google Classroom environment found that the privacy policies and legal terms governing these services are opaque, layered and inconsistent with data protection laws (Hooper et al., 2022). These policies showed that Google collects and processes a diverse range of data about children while they use Google Classroom to learn, including data processed by sensors, such as typing speed, keyboard patterns and interaction patterns with the service. However, these policies lack transparency about the purposes of processing and how each type of data is interpreted or used by Google and shared with other organisations, as made clear by the data protection impact assessment on Google Classroom carried out by the Privacy company in the Netherlands (Nas & Terra, 2021a, 2021b).

Although Google claims full compliance with data protection regulations, the socio-technical investigation suggests otherwise. We conducted the investigation first in 2022 and again in 2024.

In 2022, we investigated Google Classroom's 'Education Fundamentals' (a free version) by inviting nine and twelve-year-olds to demonstrate their user journeys on school-provided platforms while we captured the resulting data flow. Both children showed us that their teachers shared links to learning resources hosted by external services, like Vimeo and Google's additional service, like YouTube, via Google Classroom. These 'additional' services were governed by inferior privacy protection compared to Google's Education privacy policies, which guarantee no commercialisation of 'core service data' for advertising purposes (Google, 2022). Since one child had access to more additional services (such as Maps, YouTube and Hangout) than the other, it appeared that schools used different settings for Google Classroom, whether or not they knew the implications for commercial data collection.

When both children clicked on links to external services, like Vimeo, or materials in Google's additional services, such as YouTube, they did not receive any notification that

they were leaving the data-commercialisation-free zone. The data flow captured by Lightbeam showed that when the nine-year-old accessed the learning material hosted by Vimeo through the links that teachers posted, he was exposed to 42 third-party surveillance services. These services included Google's ad service and TikTok's and Facebook's analytics. When the child accessed another learning resource hosted on YouTube, the number of third-party services tracking the child's online learning journey increased to 92. The other child participant was exposed to a similar level of cookie surveillance. Such surveillance contravenes data protection regulations.

Taming Google Classroom?

In August 2021, Google agreed to implement various changes, including introducing technical controls allowing schools to block students from accessing additional services when using Google Classroom after the Dutch Data Protection Authority (DPA) threatened to ban schools and universities from using Google Classroom (Nas & Terra, 2021b).

Our 2024 update of this investigation with an eight-year-old child from the same primary school as the nine-year-old child who joined our 2022 investigation and a 16-year-old child from a different school showed that this technical improvement has also been applied in the UK. As a result, both children had access to significantly fewer Google additional services compared to our findings in 2022. In addition, when the eight-year-old child clicked on the link to a learning material hosted on YouTube while still logged in with his school-assigned Google account, his access to YouTube was blocked.

Despite these technical improvements, teachers from both schools still posted links to external (non-Google) services for students to use as part of their learning. When each child clicked on the links to these external services, they were exposed to cookie surveillance placed by various Google and non-Google third-party services. One of the external (non-Google) learning services the 16-year-old child accessed through the link that a teacher posted in Google Classroom exposed her to 170 third-party surveillance cookies that fed into the advertising technology infrastructure.

While teachers posting links to learning materials hosted in Google's additional services and other external services can be seen as a behavioural or literacy problem, this same problem can be fixed with technical solutions. One option is to block access to those services with inferior privacy protection, as Google did with the eight-year-old attempting to access learning materials hosted on YouTube using his school's assigned Google account. Arguably, a better option is to lock all the data within Google Classroom and isolate it from third-party surveillance, as appeared to be the case for Microsoft Teams when our 11-year-old participant from a different secondary school accessed external learning services through a link that the teacher posted in Teams.

The improvement resulting from the technical control changes that Google implemented following the Dutch DPA's threat to ban schools and universities from using Google Classroom (Nas & Terra, 2021b) showed that effective enforcement of data protection laws and government intervention could minimise data protection risks by design. However, more needs to be done to ensure that platforms, especially platforms with

market dominance, do not abuse their market power to facilitate the commercialisation of children's personal data while they are learning. With children's rights to inclusion, privacy, safety, education and freedom from commercial exploitation often marginalised in deliberations about EdTech and data protection regulations, it is crucial to reassess EdTech impacts and bridge the data protection enforcement gap (Day, 2022).

References

Clark, D. (2022). *Most downloaded educational mobile apps in the UK 2021*. Statista. https://www.statista.com/statistics/1266710/uk-most-downloaded-education-apps/

Cobo, C., & Rivas, A. (2023). *The New Digital Education Policy Landscape: From Education Systems to Platforms*. Taylor & Francis.

Davies, H., Eynon, R., Komljenovic, J., & Williamson, B. (2022). Investigating the financial power brokers behind EdTech. In S. Livingstone, & K. Pothong (Eds.), *Education Data Futures: Critical, Regulatory and Practical Reflections* (pp. 81-92). Digital Futures Commission, 5Rights Foundation. https://educationdatafutures.digitalfuturescommission.org.uk/

Day, E., Pothong, K., Atabey, A., & Livingstone, S. (2022). Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech. *Learning, Media and Technology*, *49*(3), 356-370. https://doi.org/10.1080/17439884.2022.2152838

DfE. (2021a). *Education Technology (EdTech) Survey 2020-21* (p. 135) [Research report]. Government Social Research. https://assets.publishing.service.gov.uk/media/621ce8ec8fa8f54915f43838/Education_Technology_EdTech_Survey.pdf

DfE. (2021b). *Guidance—Remote education good practice (withdrawn on 30 March 2022)*. https://www.gov.uk/government/publications/remote-education-good-practice/remote-education-good-practice

Google. (2022, February 10). *Privacy Policy*. https://policies.google.com/privacy?hl=en-US

Hooper, L., Livingstone, S., & Pothong, K. (2022). Problems with data governance in UK schools: The cases of Google Classroom and ClassDojo. https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf

Kerssens, N., & Dijck, J. van. (2021). The platformization of primary education in the Netherlands. *Learning, Media and Technology*, *46*(3), Article 3. https://doi.org/10.1080/17439884.2021.1876725

Livingstone, S., Pothong, K., Atabey, A., Hooper, L., & Day, E. (2024). The Googlization of the classroom: Is the UK effective in protecting children's data and rights?. *Computers and Education Open*, 100195. https://doi.org/10.1016/j.caeo.2024.100195

Nas, S., & Terra, F. (2021a). *DPIA on the use of Google G Suite (Enterprise) for Education (15 July 2020, update 12 March 2021)*. https://www.sivon.nl/app/uploads/2021/06/SIVON-Updated-G-Suite-for-Education-DPIA-12-March-2021-v1.2.pdf

Nas, S., & Terra, F. (2021b). *Update DPIA report Google Workspace for Education (2 August)*. https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf

Vaidhyanathan, S. (2012). *The Googlization of Everything: (And Why We Should Worry)*. University of California Press.

West, M. (2023). *An ed-tech tragedy? Educational technologies and school closures in the time of COVID-19—UNESCO Digital Library*. UNESCO. https://www.unesdoc.unesco.org/ark:/48223/pf0000386701