

Datafying citizens

Third-party trackers and data-as-payment in government infrastructure

HELLE SJØVAAG,^I CORNELIA BRANTNER,^{II} RAUL FERRER-CONILL,^I
MICHAEL KARLSSON,^{II} & RASMUS HELLES^{III}

^I DEPARTMENT OF MEDIA AND SOCIAL SCIENCES, UNIVERSITY OF STAVANGER,
NORWAY

^{II} DEPARTMENT OF GEOGRAPHY, MEDIA AND COMMUNICATION, KARLSTAD
UNIVERSITY, SWEDEN

^{III} DEPARTMENT OF COMMUNICATION, COPENHAGEN UNIVERSITY, DENMARK

ABSTRACT

Scandinavians are among the most datafied citizens in the world. With its digitalised welfare states, Danish, Norwegian, and Swedish e-governance infrastructures collect massive amounts of data about citizens as they search for jobs, apply for building permits, and check school calendars. In this article, we analyse the use of third-party trackers ($n = 2,761$) on Scandinavian municipal websites ($n = 745$) between 2007–2023. Mobilising the theoretical framework of universalism, our aim is to understand what kind of cost data tracking constitutes for users of digital government services. Results show that Scandinavian municipal websites are dominated by commercial trackers harvesting citizen data for advertising purposes, particularly those provided by Alphabet and Meta. We conclude that commercial user-tracking on Scandinavian municipal websites does not conform to the principle of universality, proposing 1) that governments ensure transparency of the cost incurred by these websites' data tracking, and 2) that they ban commercial tracking on municipal websites.

KEYWORDS: datafication, governance, third-party services, trackers, universalism

Introduction

The digitalisation of the Scandinavian welfare states – Denmark, Norway, and Sweden – has made digital interaction with public services increasingly mandatory (Hjelholt, 2024), with limited alternatives for opting out. This shift toward digital governance is closely tied to the broader trend of datafication, or “the process of rendering into data aspects of the world not previously quantified” (Kennedy et al., 2015: 1) – key to governance developments globally (Kaun & Dencik, 2020). Advocates argue that datafication enhances government transparency, efficiency, and effectiveness (Andrews, 2019), while also “datafying” citizens (Hintz et al., 2018) to improve governance, citizen services, and trust (Flyverbom, 2017). The global infrastructures that enable datafication are driven by the same tech companies that datafy media systems, such as Alphabet, Meta, and Microsoft. The private and commercial ownership of critical data infrastructures thus pose profound challenges to the normative foundations of the Nordic welfare societies (Jakobsson et al., 2024; Jørgensen, 2024) – traditionally founded on principles of inclusion and diversity (Sjøvaag & Ferrer-Conill, 2024a).

At the same time, datafication drives an evolution from the traditional notion of a media welfare state (Syvertsen et al., 2014) toward a “data welfare state” (Andreassen et al., 2021; see also Kaun & Löfgren, 2024), which in a Scandinavian context would require a fair, unbiased, and decommodified processes of datafication free from commercial logics. Hence, in datafied societies, key public institutions become subject to the data logics (Fourcade & Gordon, 2020) that govern the platform economy (Hintz et al., 2018), raising concerns about the extent to which governance can remain independent of corporate influence, and about data use, ownership, and control. At the same time, governance itself becomes shaped by the logic of data collection, automation, and algorithmic prediction, rather than by legal–bureaucratic categories alone (Fourcade & Gordon, 2020).

One mechanism of datafication is tracking (Andreasson et al., 2021). Most of the tracking necessary to support datafication is conducted by third-party services (TPSs) owned by private, commercial companies (Helles et al., 2020). Research has critically interrogated these processes as acts of surveillance (Andrejevic, 2013) or monitoring (van Dijck, 2017) that erode the transparency of governance (Redden, 2018). Beyond the issue of privacy, the key issue here is who really benefits from cookie-harvested citizen data through e-government services. As public service infrastructures, government websites are tax-funded portals to a range of essential services and databases that citizens are compelled to use. Embedded with commercial tracking functions, these infrastructures have amassed large amounts of citizen data over time – data that they are essentially giving away for free to TPSs.

Data tracking can therefore be considered a cost of use, as data assume a form of currency (van Dijck, 2014) or capital (Sadowski, 2019) in the platform economy (Hintz et al., 2018). While such services will often remain functional if non-essential cookies are declined, research suggests (Utz et al., 2019) that many

users are unaware of the extent of data collection and the implications of their consenting to data tracking. Moreover, despite the regulatory requirements set by the General Data Protection Regulation (GDPR), many websites still collect user data without explicit user consent, even when users can reject such tracking (Berens et al., 2024; Götze et al., 2022). The dominance of commercial actors in this domain thus suggests that tax-funded online services are facilitating the monetisation of citizen data. To understand what this cost entails, we mobilise the concept of universalism – a founding principle of the welfare state (Syvertsen et al., 2014) whereby all citizens are equally entitled to the services of the state (Esping-Andersen, 1990).

A key aim of universalism (Kildal & Kuhnle, 2005) is to emancipate citizens from the negative consequences that market and class mechanisms can have on wealth distribution. Government services should ideally work as levelling instruments to equal peoples' opportunities in life (Esping-Andersen, 1990). Universal access policies (Mossberger, 2008) constitute concrete expressions of this aim, ensuring that all citizens, regardless of their abilities, are able to use public services. This has a number of manifestations in public service provision – from the design of buildings to accommodate wheelchair access to automated voice-over translation on radio and digital accessibility (European Union, 2016). In cases where essential services such as railways, electricity, and Internet access are provided by private companies, universalism means equal access at a fair price, without refusal of service or quality differentials (e.g., Ministry of Digitalisation and Public Governance, 2023–2024). Welfare state governments often regulate markets for essential services (Kammer, 2016) so that the cost of using them does not exacerbate socioeconomic differences in society or exclude someone from service. The “cost” of use typically extends beyond direct payments in these political systems. Many services carry indirect costs through taxation, whereby governments subsidise public goods including museums, swimming pools, and roads, where individuals pay a small fee for direct use.

Digitalisation suggests that increasingly, there is also an indirect cost associated with the use of essential digital services in the form of personal data, expanding the economics of universalism to include datafication: the collection and analysis of information to produce knowledge, improve services, and generate economic value through data (Mayer-Schönberger & Cukier, 2013). A whole industry of trackers, cookies, and other TPSs has emerged to capitalise on this data economy (Libert & Nielsen, 2018), whereby personal data collected from users can be monetised for other purposes, including personalisation of content, targeted advertising, psychometric profiling, and analytics (Helles et al., 2020). The presence of tracking technologies thus amounts to an added cost of service that users pay when visiting websites, as their data is continuously collected and repurposed, including on government websites (Götze et al., 2022). When welfare states allow commercial trackers on their digital portals, this could be seen as an instance of digital capitalism (Sadowski, 2019), whereby citizens' data are monetised through these platforms.

In this article, we evaluate whether data-as-payment (Sadowski, 2019) is imposed on Scandinavian municipal websites. We furthermore consider whether this can qualify as a “fair price” that citizens pay when accessing portals containing essential information about government services, such as health and sanitation, local democratic procedures, and social services that municipalities provide. As e-governance policies increasingly push users towards digital solutions, we examine to what extent municipal website tracking aligns with the principle of universality (Kildal & Kuhnle, 2005). To address these issues, we explore three research questions:

RQ1. What tracking functions are employed in Scandinavian municipal websites, and how have these functions evolved over time?

RQ2. What kind of cost does this tracking entail for citizens?

RQ3. To what extent do Scandinavian municipal websites and their embedded data infrastructures undermine the principle of universality by imposing hidden costs on citizens through data tracking?

We ask these questions in the Nordic context of Scandinavia, a region covering approximately 20 million inhabitants in Denmark, Norway, and Sweden. Their citizens’ high levels of trust in public institutions and acceptance of data collection (Andreasson et al., 2021), their digitally innovative public sectors (Broomfield & Reutter, 2022), as well as their regulation-oriented welfare state systems (Jakobsson et al., 2024), provide an apt case for testing how universalist principles harmonise with the principles of datafication. Our analysis is based on a survey of the TPSs ($n = 2,761$) found on 745 municipal websites from the three countries between 2007–2023, adding much needed empirical data to questions regarding the datafication of citizenship. Findings show that most TPSs found serve the commercial interests of the largest actors in TPSs, particularly Alphabet and Meta. We thus add to the discussion of how trackers, as part of the infrastructure of datafication, contribute to datafy citizenship.

Tracking the datafied citizen

Historically, states have collected data on citizens to inform the bureaucratic organisation of society (Flensburg & Lomborg, 2023), using this information to understand, predict, and to some extent also control citizens (Hintz et al., 2018). Scandinavian welfare states have been particularly keen to embrace datafication technologies in public administration and public policy development (Kaun & Dencik, 2020), shaping the “future imaginary” of the welfare state (Broomfield & Reutter, 2022). As Broomfield and Reutter (2022: 5) have remarked, “the Nordics are regarded as data goldmines with massive amounts of high-quality granular data on citizens”. Indeed, as Barassi (2019: 419) argued, the digital welfare state relies on “the systematic coercion of digital participation”, where citizens must engage with data technologies and give up their personal data in

exchange for government services – services they have already paid for through taxation. Integral to this process of datafication is an ecosystem of platforms and applications that collect and host data (Sadowski, 2019), with tracking technologies playing a central role in data transfer and analysis.

Trackers form a key part of this infrastructure as TPSs augment the capacity of the first party in some way by transferring user data to an outside entity (Pybus & Coté, 2022). There are several studies on trackers that examine their use on websites from a long-term perspective, consistently finding a steady growth in their usage until 2018 (Helles et al., 2020). Tracking is conducted through various methods, historically relying on cookies and JavaScript as the primary means of monitoring user behaviour on the worldwide web. Some of these functions provide clear benefits to users, including functionalities, multi-device browsing, and personalisation. The prevalence of web tracking varies across the globe, and despite legal efforts for strengthening privacy (such as GDPR), violations are common, which calls for more effective compliance, monitoring, and enforcement tools (Samarasinghe & Mannan, 2019). This constant and continuous tracking of (meta)data for unstated purposes is behind Clarke's (1988) concept of dataveillance. At its core, dataveillance is "a far-reaching proposition with profound consequences for the social contract between corporate platforms and government agencies on the one hand and citizens-consumers on the other" (van Dijck, 2014: 255). Fuelled by datafication, it entails an accumulation of information for data-driven decision-making (Constantinides et al., 2018), whereby data serve as building blocks for new information (Kitchin, 2014), often for economic purposes (Mejias & Couldry, 2019).

User data is therefore not only a form of currency within the realm of datafication (van Dijck, 2014), but also a cost borne by users, with its proceeds enabling data industries to reinvest in the development of new products and services. In this sense, citizens tend to understand that they "pay" for free services as companies harvest their private data (Fehrenbach & Herrando, 2021). The data rendered by users visiting municipal platforms must be considered highly valuable in the aggregate, particularly for platform companies like Google, whereby their analytics capabilities benefit from the type of behavioural data that municipal services render – browsing behaviour that indicate a person's marital status, financial situation, property ownership, employment history, and health status. If such analytics services were in place, this could put citizens in a weak position in terms of the cost of using online municipal services. While tracking functions such as Google Analytics offer free tracking services to the website, governance-enhancing functions such as accessibility and feedback are usually paid-for services that require heavy subsidy on the user side. This distinction is significant because the value generated through the platform varies depending on their function, which is why we operationalise "cost" as the data tracking that citizens incur when using municipal services.

Regardless of economic valuation, there is a cost associated with datafication, not only for the user but also for actors hosting data-gathering applications, who must navigate new issues of transparency, ethics, and compliance as they

manage increasingly complex relationships and partnerships (Sjøvaag & Ferrer-Conill, 2024b). Indeed, the constant disclosure of dataveillance tactics in online government agencies can undermine citizen's trust in state agencies (van Dijck, 2014). Moreover, when users of these services are profiled as both citizens and consumers, the infrastructures of datafication serve to blur the boundaries between private and public (Barassi, 2019), particularly as consumer data are also tracked when users act as citizens rather than as consumers. Research on G20 government websites has shown that trackers are indeed present in public-sector digital infrastructures, and that third-party-cookies are added even when users do not provide consent (Götze et al., 2022). However, little is known about the extent and function of online tracking within the back-end of the Scandinavian public administration online infrastructure, particularly on the municipal level.

Here, we define functions as the purpose for which data is gathered, including for commercial purposes such as advertising, as well as potentially beneficial governance-enhancing tracking functions such as interaction and analytics, alongside technical functions such as consent, delivery, and audio–video playback. We understand cost as incurred by users when data are tracked (and potentially traded), whether knowingly or unknowingly, in exchange for a product or service that is seemingly “free” and, in the case of municipal websites, is noncommercial and publicly funded. This cost remains unknown (Elvy, 2017: 1384) and largely invisible to users. Fairness is understood as the extent to which costs are informed and distributed equally under the structural conditions (Fourcade & Gordon, 2020) of the data welfare state.

Tracker regulation and the provision of universality

Most attempts to manage dataveillance and its potential effects have been through regulation. However, research on the impact of the GDPR, which has been in effect since May 2018, presents mixed results regarding its influence on tracker usage. Overall, the GDPR has had a relatively low impact, with only minimal changes in the number of trackers following the law's implementation (Rughiniş et al., 2021). Moreover, a substantial number of websites either cannot or do not fully comply with GDPR regulations (Hu & Sastry, 2019). There is also evidence that tracking entities may still be able to monitor user behaviour, even after users have explicitly declined cookies (Sanchez-Rola et al., 2019).

Considering the challenges of regulation, this study proposes universality as a relevant, yet underexplored framework to understand how datafication impacts and challenges the concept of citizenship (e.g., Broomfield & Reutter, 2022; Hintz et al., 2018; Kaun & Dencik, 2020). Essentially, universalism is attached to the benefits and services to which all citizens are entitled (Kildal & Kuhnle, 2005). As a cornerstone of welfare economics and the welfare state, universalism mobilises the idea that universal access to certain services benefits labour and production as well as the citizen and the state alike. Access to health and education, recreational services like parks and libraries, as well as transport and communication services, is thought to produce healthy, knowledgeable, and

happy individuals whose resulting productivity benefits the economy as well as the capitalist owners of production (Esping-Andersen, 1990). Universalism is also intended to reduce social inequalities, ensuring that all citizens have equal opportunities, irrespective of market forces or class structures.

Since the 1990s, many universal services have undergone privatisation, including railroads and postal services, energy provision, and telecom. This shift has seen the state moving from owning such essential services to regulating them (Syvertsen et al., 2014). Because these markets are often served by monopolies due to their high investment needs, transparency and oversight are implemented to ensure their legitimacy and trust among the public (Kaun & Dencik, 2020; Redden, 2018). Universalism is important in this regard because it ensures that no one can be excluded from these services. While monopolists could, in principle, set arbitrary prices, regulation ensures that essential services like water, sanitation, transport, and Internet access remain affordable and accessible to all. Many universal services thus function as infrastructures that blur the distinction between citizen and consumer, with universalism maintained through state intervention and regulation.

Municipal websites are portals to many essential services that citizens need on a daily basis. They provide sanitation services, transport information, social services, and recreational services, as well as oversight of local policy processes. They are also portals for a range of important functions, including employment opportunities, applications for financial support, building permits, local taxation forms, and kindergarten and school intake. Citizens pay for all these digital services through their taxes, which is transparent and traceable through public budgets. However, they would also bear additional, hidden costs in the form of data extraction if (first- and third-party) trackers were embedded in the website's infrastructure, for both commercial and administrative purposes. While the cost of taxation is transparent and subject to citizen oversight, the data cost incurred from using these services is not. The first cost lies under the jurisdiction of the state and is thus subject to public legitimacy, while the second lies beyond the jurisdiction of the state and remains opaque. If municipal websites embed tracking technologies that collect personal data for TPSs, this would introduce a largely unaccounted-for cost. However, the extent to which such tracking occurs, whether for commercial, administrative, or analytical purposes, remains uncertain. As citizens are increasingly compelled to interact with digital platforms, this raises important questions about the nature of these interactions and their implications for universalism. If tracking mechanisms are indeed present, do they constitute a form of "forced compliance" (Barassi, 2019) with private data infrastructures?

Data and methods

The research design contains three steps. First, we compiled a list of 745 municipal websites from Denmark (98), Norway (357), and Sweden (290). The dataset was compiled through archive.org, a web archive that focuses on front-end systems due to the availability of their digital footprints. Second, we

identified a total of 14,740 TPSs. Of these, 2,761 occurred on more than one website. A file was compiled tabulating how many times each TPS occurs in the dataset for each year spanning 2007–2023, and how many different URLs they occur on, amassing multiple entries for each URL. The list was deduplicated so that double entries such as “www.instagram.com” and “instagram.com” are not treated as two different trackers.

Third, we classified all trackers appearing more than four times in the dataset (about 1,500 trackers) using algorithmic approaches to the largest openly available registry of tracker functionality and ownership, which is the whotracks.me dataset, by automatically extracting relevant data. We manually vetted 250 of the most frequent values to assess the quality of the classification. The vetting showed that most trackers were classified correctly while a few were re-coded to more accurately reflect their function, for example, from “customer interaction” to “audiovisual services”. From this process, we deductively created our universe of functions, reflecting the purpose for which data is gathered; the coding scheme consists of ten categories (see Table 1). Functions were coded as either commercial (primarily advertising), administrative (including consent and audio–video playback), technical services (hosting and content delivery services (CDNs)), essential services, extensions, customer interaction, analytics, and links. We then used our codebook to manually code the 100 most prevalent trackers in each country. Intercooder reliability was attained through a process of primary and secondary coding, whereby the initial coding was hand-checked by subsequent authors until we arrived at agreement. In this coding process, we also classified the ownership of trackers and their private/public domain, using a combination of the whotracks.me and whois, whereby the top 100 were also checked manually.

Table 1 Operationalisation of tracker functions on Scandinavian municipal websites

Function	Operationalisation – cookies and scripts from companies engaged in provision of:
Advertising	placement and targeting of web advertisements (e.g., Google Ads)
Analytics	traffic measurement and website performance optimisation (e.g., Google Analytics)
Content delivery network (CDN)	hosting for bandwidth-intensive content (excluding audiovisual content) or standardised web functionalities (e.g., Akamai, Google Hosted Libraries)
Audio–video playback	hosting and delivery of audiovisual content (e.g., YouTube)
Essential	core functionalities necessary for website operation (e.g., Cloudflare).
Extensions	extra features or integrations to websites (e.g., reCAPTCHA).
Customer interaction	features for user engagement and support (e.g., Zendesk).
Consent	management of user consent and privacy preferences (e.g., Cookiebot).
Link	services for redirections or embedding of content, (e.g., Bit.ly)
Hosting	infrastructure for website storage and delivery (e.g., Amazon Web Services)

The analytical procedure involved first inferring what type of data is collected from the functions operationalised, then inferring data-as-payment from the functions. The advertising function refers to data collected via cookies from ad-centric companies such as Google (Alphabet), Facebook (Meta), LinkedIn (Microsoft), Twitter (now X), and TPSs from technology companies such as Amazon and Oracle, which derive part of their revenue from advertising. Since these municipal websites are legally prohibited from monetising their traffic through on-site display advertising, the municipalities do not use these TPSs to generate profit. Rather, they likely do so for communicative purposes, for example, to appear approachable or to inspire users to share content to their own social media profiles. The net result, however, is that the TPS providers can subsequently use the collected data to match users with vendors outside the municipal sites. The analytics function collects data for marketing, management, and optimisation purposes. These TPSs are integral to site analytics, which entails monitoring websites in order to improve the user experience of the site. In its contemporary form, this involves collecting data on the interaction between users and site, sending it back to the provider of the analytics service, and subsequently presented to the municipal web operator in a standardised, aggregated form.

The content delivery network (CDN) function provides publishing and web feature services. This serves a number of purposes. CDNs are often used to alleviate the display of bandwidth-intensive content such as video. Rather than having users download a video from the municipality's own server, the file is placed on a third-party-operated server (e.g., YouTube), whose infrastructure is optimised for high-bandwidth traffic. CDNs are also used to ensure consistency in website features, such as fonts, stylesheets, and JavaScript, since embedding this information via a stable online repository (the CDN) offers greater reliability than embedding it directly within the site itself. However, since CDN functionality is often ubiquitous across a website, and because the CDN marketplace is concentrated on very few players (Sjøvaag et al., 2024), CDN providers are often in a good position to collect detailed information about users' behaviour on and across many different sites.

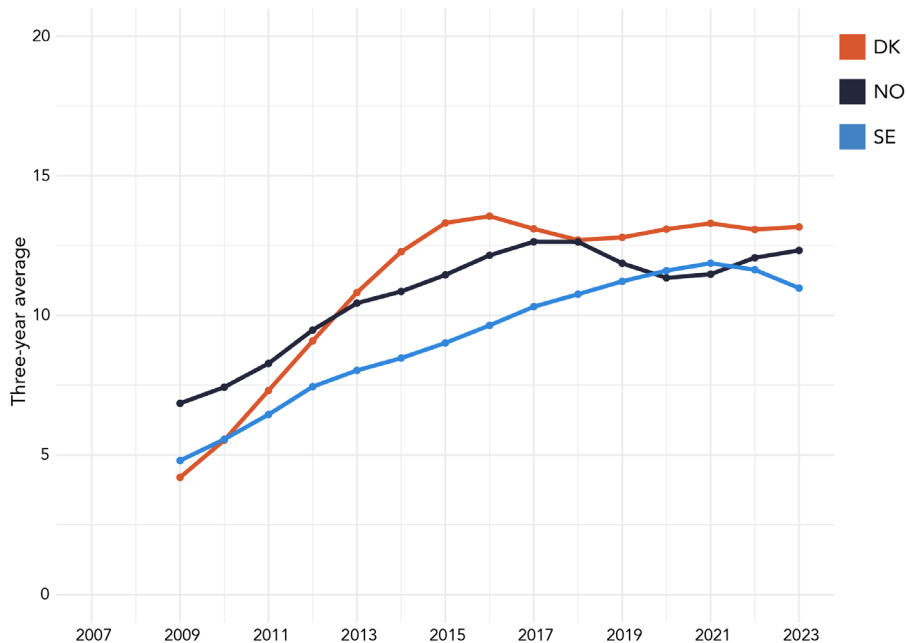
The same applies to functions such as cookie consent forms, hosting, and audio–video playback. These also facilitate typical and necessary functions on the website, while simultaneously allowing providers to collect tracking data. A special category in our coding scheme is the link function, which refers to a recurrent use of the TPS infrastructure to provide links to other websites, almost exclusively those of other municipalities. Here, trackers perform administrative functions, for example, linking to neighbouring municipalities, while also facilitating data collection on users. The customer interaction function typically provides facilities for users to provide information at a site, for example, by filling out surveys or reporting errors. Extensions provide additional services like embedding and displaying information from job portals, weather, and translation services on the site. Essential functions refer to exclusive or monopolised services, such as the provision of interfaces to other public services, for example, allowing

people to fill out forms on a government portal. Hence, these TPSs provide a variety of functions, but they all collect data on users that can be used for analytics purposes beyond those needed for the function itself.

Results

The analysis shows that TPSs are used by all municipalities in Scandinavia. Figure 1 displays the rolling mean of the number of TPSs per site in each country. TPS use increases over time across countries, yet there is some variation between countries. The level in Denmark is higher from 2012 onwards, and the level in Sweden is the lowest. The use of TPSs grows at similar rates in Norway and Sweden and faster in Denmark, where it also peaks earlier, and all countries have seen some drop (or levelling off) in the number of TPSs used at some point since 2014. However, the figure clearly documents that municipalities persistently rely on TPSs.

Figure 1 Three-year rolling average of third-party services per site in Denmark, Norway, and Sweden, 2007–2023



Comments: Data includes TPSs that occur on more than one municipal website.

Figures 2–4 show the evolution in the footprint of the 25 TPSs that have the highest footprint in each country at any time between 2007 and 2023. The footprint refers to the percentage of national municipalities that a TPS reaches. The TPSs are ordered from top to bottom by their average footprint across the years they were in use. Here, we see substantial differences between the countries. In Denmark and Norway, nine and seven of the top-ranking TPSs, respectively, are nationally operated, while this is only the case for three in Sweden, which is a significantly lower proportion [$2 (1, N = 76) = 3.97, p = .046$] (w. Yeats’s correction).

Figure 2 Heatmap of top 25 trackers in Denmark, 2007–2023

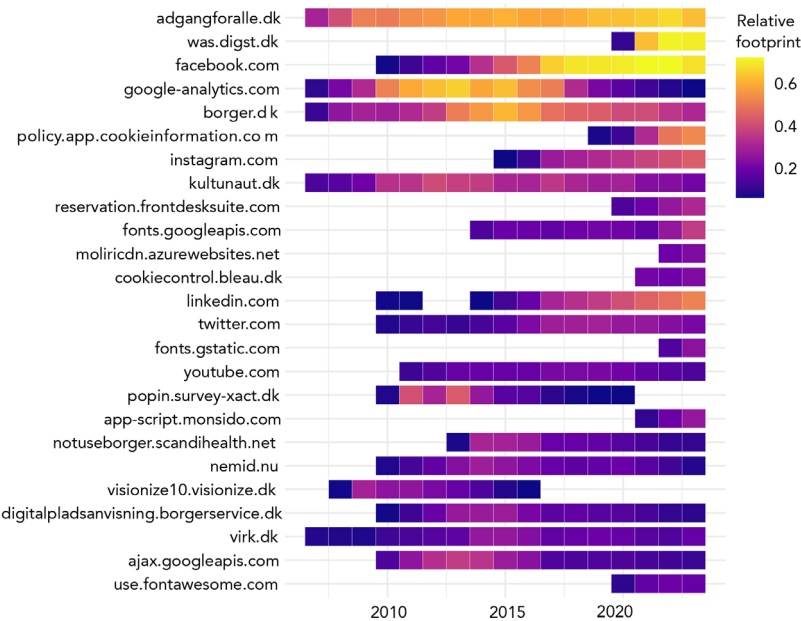


Figure 3 Heatmap of top 25 trackers in Norway, 2007–2023

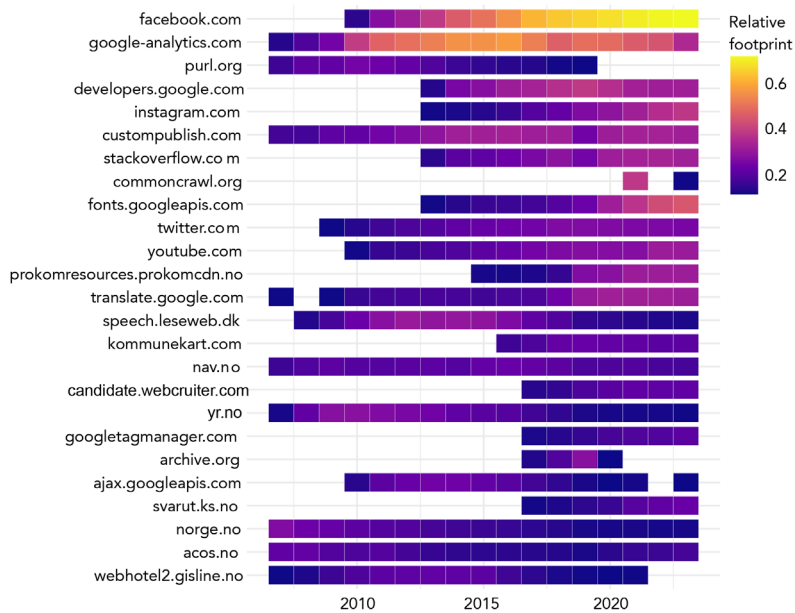
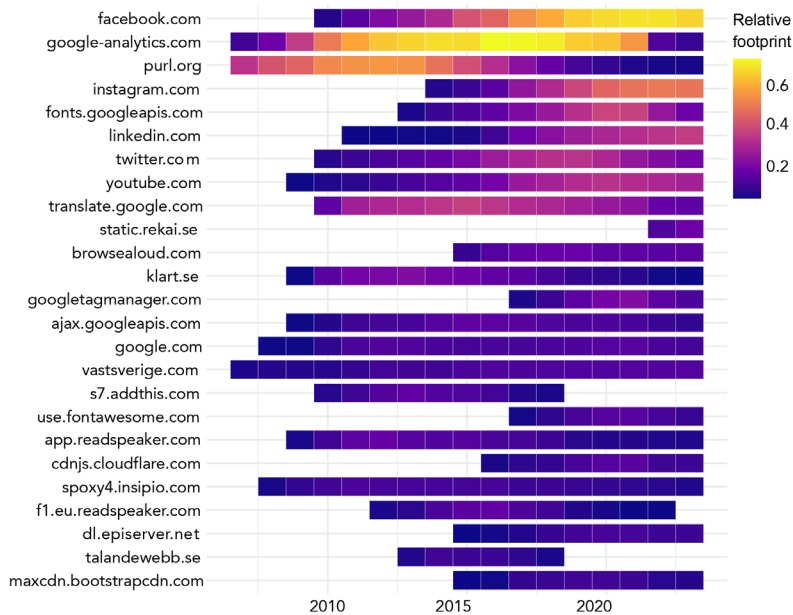


Figure 4 Heatmap of top 25 trackers in Sweden, 2007–2023



Figures 2–4 also suggest substantial, temporal fluctuations among the popular TPSs. Some of the services that were highly popular early on, such as purl.org in Norway (#3) or survey-xact.dk in Denmark (#17) have since gone completely out of use. In some respects, this is to be expected. The way websites are hosted and operated has shifted from a largely server-based architecture with static content structures to dynamic hosting in content management systems, just as expectations of the interactive affordances of websites have also changed. The pattern of adoption, rejection, and replacement also reflects larger trends in the use of TPSs, in particular a growing penchant for services operated by global corporations. In the following, we illustrate this with two examples.

A high-level illustration of the dynamics related to global providers can be seen in the use patterns that characterise services, in particular, several of the services provided by Meta and Alphabet. Figures 2–4 show that services operated by these companies – such as Google Analytics, YouTube, Facebook, and Instagram – are among the most common TPSs in municipalities in all three countries. Figure 5 displays the combined footprint of all services provided by the two companies, illustrating the maximum reach of each service. If a website includes any or all TPSs from one company, it counts as a single site in the company’s footprint. The figure shows how their footprints have changed over time.

Figure 5 Google and Facebook TPS prevalence, 2007–2023

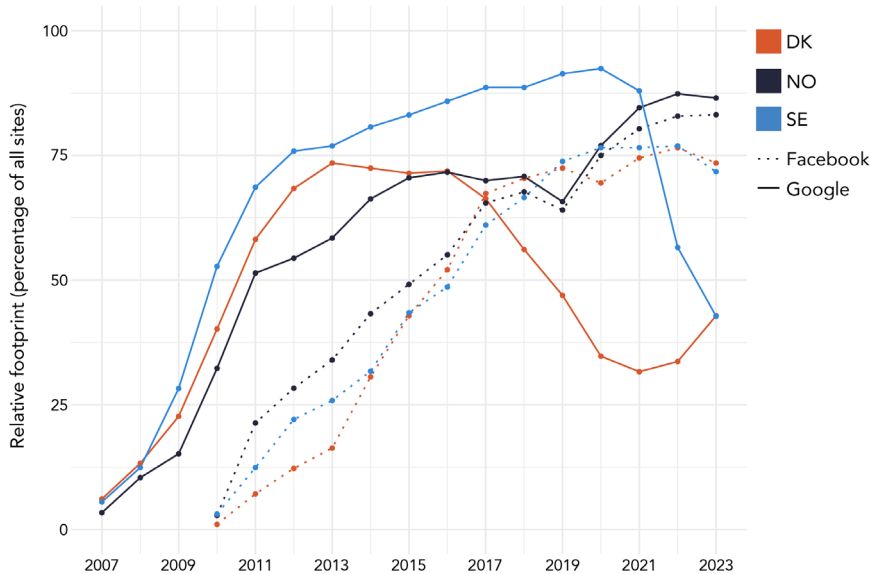


Figure 5 shows a reduction in the use of Alphabet's services on Danish municipal sites since 2013. Alphabet's footprint declined from 78 per cent in 2013 to around 32 per cent in 2021, followed by a slight increase. Their prevalence in 2023, at 43 per cent, still represents a reduction of about 35 percentage points since the highest point in 2013. In Sweden, the footprint of Alphabet also dropped, from 93 per cent in 2020 to 45 per cent in 2023, that is, it more than halved. In Norway, we see a remarkably different development with an almost continuous growth, with the highest footprint registered in 2022 at 87 per cent. An early driver of the presence of Alphabet services is Google Analytics, the decay of which also largely accounts for the drop in Alphabet's combined footprint. Country-level differences in municipal websites' use of Google's services indicate that the debate on, and implementation of, GDPR (in effect from 2018) led municipalities to scale back their reliance on Alphabet TPSs at different stages and on different levels. Here, the effect of GDPR in Denmark has led to an outright ban on Google Analytics on public sites in 2024, but the service has been the topic of public debate and criticism since 2015. The later uptick in use of Alphabet services in Denmark since 2021 is largely driven by increased reliance on the content delivery services provided by the company, in particular Google Fonts. In Sweden, there has been a downturn in use of several of Alphabet's services, but the major reduction was caused by a drop in the use of Google Analytics, starting around 2016.

In contrast, the development of Meta's TPSs across the three countries shows greater similarity, marked by growth. Both Denmark and Sweden saw Meta's footprint on municipal websites reach around 75 per cent in 2018, where it has remained since. In Norway, Meta's presence has risen slightly faster and sits at a higher level toward the end of the period, showing no signs of leveling off.

Regarding potential explanations for these results, the transition – first from traditional websites to Web 2.0. (Sjøvaag et al., 2016), and subsequently to public bodies actively maintaining Facebook and Instagram profiles – appears to be a likely factor. Indeed, municipalities in the three countries incorporate the interactive affordances of social media, and they have developed sophisticated, communicative repertoires for using them effectively (Baltz, 2020). Despite the democratic potentials of expanding dialogue between citizens and municipal administrations, the presence of Meta's trackers on municipal websites also showcases the cost of this connection, as their trackers collect information that further fuels their advertising model (Libert & Nielsen, 2018).

The changing landscape of trackers

At the capillary level, the adoption and discontinuation of different TPSs is highly diverse. To map out consistent trends, the 100 most common TPSs can be compared. Here, we compare the development in the prevalence of different TPS categories in the three countries between 2010 and 2023. Our 2010 starting point was chosen to account for the establishment of dynamic web as a norm (Barker, 2016), to ensure that comparisons are not distorted by the differences between static and dynamic websites. The development in the use of these TPSs is shown

in Figure 6. Each row corresponds to a function category, and the bars show the development in use between 2010 and 2023. The prevalence is measured as the share of sites where a category is present at the two points in time.

Figure 6 Prevalence of TPS categories, 2010–2023

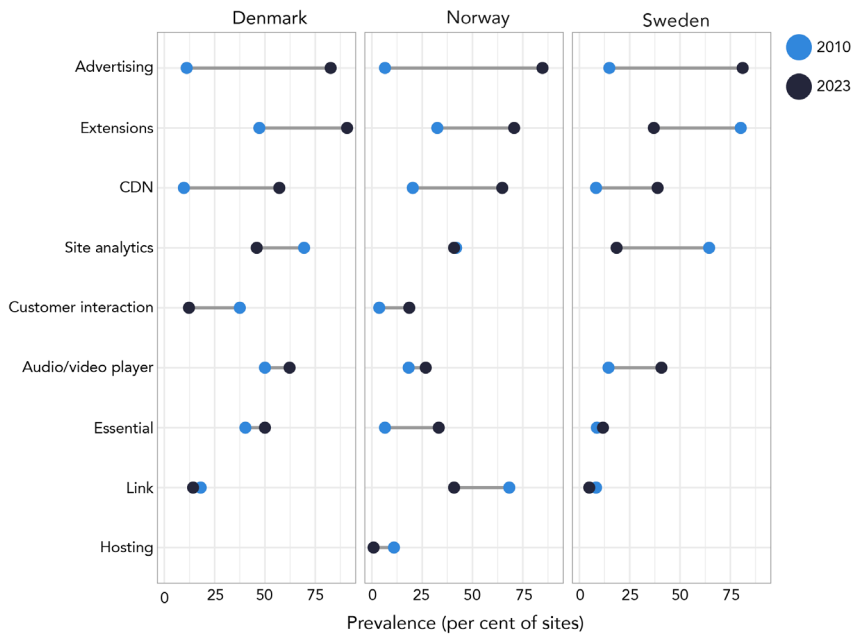


Figure 6 shows that the advertising and CDN categories have seen substantial growth between 2010 and 2023, and site analytics have seen minor drops. The drop in site analytics reflects the rejection of Google Analytics, but not necessarily that site analytics is used any less. Given that the figure includes the 100 most common TPSs, results show that no unified alternative has established itself as the preferred replacement for Google Analytics. It may also suggest that site analytics is provided by the hosting services or content management systems used by municipalities.

Advertising TPSs have grown from near zero being present on around 75 per cent of sites. This is predominantly driven by the advent of TPSs provided by various social media companies (further illustrated in Figures 2–4), but the expansion also covers other services, such as Oracle’s AddThis. Hence, the discontinuation of Google Analytics due to privacy concerns has not manifested as a more generalised restriction on TPSs that erode privacy. In conjunction, the modest decline in site analytics and the strong growth in advertising functions suggest that regulation is applied on a case-by-case basis. Only when something is deemed completely unacceptable is it restricted. When devoid of controversy, however, it is used freely.

The development of CDN services is also relevant to our discussion. The growth in this category comprises several different intertwining trends. The first is illustrated in Table 2, which shows the CDNs that have grown the most in each country.

Table 2 Top five CDNs by growth in Denmark, Norway, and Sweden, 2010–2023

	Denmark	Norway	Sweden
1	fonts.googleapis.com	custompublish.com	fonts.googleapis.com
2	code.jquery.com	fonts.googleapis.com	cdnjs.cloudflare.com
3	fonts.gstatic.com	prokomcdn.no	dl.episerver.net
4	cdnjs.cloudflare.com	code.jquery.com	use.fontawesome.com
5	cdn.jsdelivr.net	visbrosjyre.no	ajax.googleapis.com

In Denmark and Sweden, all the top CDNs represent global service providers that are market leaders in their segment of CDN provision. Two of the top services (one in Norway) are provided by Alphabet (gstatic and googleapis). The only local CDNs to make the top five are visbrosjyre.no and prokomcdn.no in Norway.

At one level, the growth in CDN services reflects a general trend in web development, whereby websites increasingly rely on standardised service delivery. For instance, the rise of the JQuery repository (a common library used in the implementation of website functionalities) reflects an increased standardisation of code, ensuring a higher degree of consistency and security. While the alternative – relying on local caches or code snippets – entails less streamlined implementation, it also provides potentially better privacy. Relying on global, centralised repositories invariably invites the collection of tracking information. While Google Analytics has been largely discontinued, other services by the same company are still widely used. Alphabet’s services ostensibly provide gainful services to web managers and users alike; however, they are clearly not “free”, as they collect data on users. Hence, from the point of view of information flows facilitated by TPS implementation, the use of standardised services is questionable. However, choosing a global CDN provider also aligns closely with key values in municipal service provision – delivering smooth, professional websites that offer consistent quality, aesthetics, and functionality across different browsers and devices (both handheld and desktop) aligns closely with universalist ideals of universal access.

Hence, to answer the first research question – What tracking functions are employed in Scandinavian public administration websites, and how have these functions evolved over time? – commercial and technical functions dominate, and global standardised technical functions, particularly CDNs, have increased in prominence over time. Tracking for advertising purposes continues to proliferate, despite the discontinuation of Google Analytics, illustrative of the platform economics at play in the TPS domain.

The cost of being tracked and the principle of universality

Like most websites, municipal sites in Scandinavia deploy a range of voluntarily installed (Helles et al., 2020) social media and third-party trackers (Götze et al., 2022), and they continue to grow in numbers (Su et al., 2023). As government and corporate platforms meet on these municipal services, citizens are turned into consumers (van Dijck, 2014) through a process of “dataveillance” (Clarke, 1988), whereby user consent renders citizen data into capital (Sadowski, 2019) that citizens exchange as a form of payment for these services. If an increased extraction of data can be equalled with increased cost, then the results suggest that this cost has increased over time in all three countries. At the start of the time series, there is a rather sharp increase in TPSs in all countries, but that levels off from 2015 onwards. With a few exceptions, most trackers stem from .com domains and originate from big American companies (i.e., Alphabet and Meta). The most prominent TPSs belong to the major platform companies and advertising trackers. Furthermore, these TPSs went from near absent to widely spread. In general, it appears that trackers have increased the “systematic coercion of digital participation” (Barassi, 2019: 419) of citizens throughout Scandinavian municipalities over time. While citizens may understand that they “pay” for services with their data (Elvy, 2017; Fehrenbach & Herrando, 2021), the presence of such economics within welfare state services could also serve to decrease citizen trust in digital government services (van Dijck, 2014), given their low transparency (Kaun & Dencik, 2020). As an infrastructure of datafication, TPSs thus constitute a blurring of public–private value creation (Pybus & Coté, 2022). States not only collect data for the efficient bureaucratic organisation of society (Flensburg & Lomborg, 2023), but the “data goldmines” (Broomfield & Reutter, 2022) that these websites enable also put most of the cost (Coyle, 2018) on the user.

On Scandinavian municipal websites, tracker data constitute payment in two ways. First, citizens pay with their personal data. TPSs collect data on citizen users as they link to other websites, render functions, perform analytics, and foster interaction and accessibility. Second, citizen data constitute a subsidy that users provide in exchange for external services that municipalities would otherwise have to develop in-house. These services – like maps, weather, read-out, or design – would otherwise incur a taxable cost to e-governance. Hence, citizen data provide a savings opportunity for the municipalities. In both cases, the cost is indirect. To that end, the cost of use is really unknown (Elvy, 2017). This is problematic in a welfare state context because transparency and oversight are key to ensuring citizen trust in monopolised sectors like municipal portals to welfare services (Redden, 2018). While GDPR and end-user licensing agreements (Sadowski, 2019) render some level of control to the user, tracking can occur regardless of consent (Berens et al., 2024). Moreover, the presence of trackers remains in the control of the host. TPS tracking on municipal sites, and the data transfer that this entails, thus constitutes “forced compliance” (Barassi, 2019),

which challenges the principle of universal access as well as the transparency of digital governance. To answer the second research question – What kind of cost does this tracking entail for citizens? – data-as-payment satisfies mainly commercial goals, suggesting that municipal websites also facilitate a platform function for TPSs in the digital economy (Gillespie, 2018).

A notable exception here is the inclusion of accessibility trackers like *adgangforalle.dk* – a read-out function developed by the Danish Agency for Digitalisation. As the top tracker on Danish municipal websites, *adgangforalle.dk*, as well as similar services found on Norwegian and Swedish municipal websites such as *leseweb.dk* in Norway, constitute audio–video functions designed to accommodate universal access provisions mandated by European Union regulation (European Union, 2016). *adgangforalle.dk* is not only found on all Danish municipal websites, it also exemplifies a TPS developed and maintained by the public sector, without commercial incentives (e.g., Ranchordas & Scarcella, 2021). However, such universal access features are also provided by private commercial operators, such as Google Translate, or BrowseAloud and ReadSpeaker, which feature on Swedish municipal websites. As commercial alternatives can accommodate such universal access, private vendors also exist within this market to mitigate the public costs of digital infrastructure provision.

Universalism reflects the principle that certain services should be available to all citizens regardless of their income and social status (Kildal & Kuhnle, 2005), to support equal opportunity (Esping-Andersen, 1990). In cases where universal provision has been willingly transferred by the state to the private market, welfare states ensure that these operate under universalist principles through regulations (Syvertsen et al., 2014), chief among which is equal access and fair pricing. To explore this, the third research question asked: To what extent do Scandinavian municipal websites and their embedded data infrastructures undermine the principle of universality by imposing hidden costs on citizens through data tracking? The findings show that data tracking constitutes an added, hidden cost that citizens incur when they change their address, seek building permits, apply for public sector jobs, or check the school calendar. The embedded data infrastructures of Scandinavian municipal websites could thus be said to substantially undermine the principle of universalism, as they facilitate the market power of commercial, advertising-driven interests, Alphabet in particular. On the other hand, certain costs of running digital government services have been willingly transferred to the private market, whereby citizen data subsidise universal service. Universal access is also largely supported by the user data collected by global TPSs like CDNs by ensuring quality of service to the user. While this practice may align rather well with privatisation efforts within welfare state systems (Syvertsen et al., 2014), questions remain as to their regulation. While citizens can opt out of data tracking for purposes other than administrative functions on these sites, citizen data constitute a subsidy, whether it is realised or not.

So, is this a “fair” cost? Fairness, in this context, is not simply about individual choice but about the structural conditions under which choices are made. Following Fourcade and Gordon (2020), fairness must be understood in

relation to the power asymmetries between states and private corporations in the data economy. From a distributive fairness perspective, the question is whether the costs of digital governance – whether financial or data-based – are borne equally by all citizens. From a procedural fairness perspective, it is a matter of whether citizens are fully informed about how their data is extracted, processed, and monetised (e.g., Hokka, 2022). Yet, the designers of municipal websites themselves may not always be fully aware of third-party tracking (Götze et al., 2022). Indeed, website design over the period covered here follows a relatively path-dependent trajectory whereby web architecture itself becomes more and more embedded with data tracking functionalities. Moreover, the sunk cost of skill development tied to free software provided by third parties enforces this path further. However, if Scandinavian welfare states are to uphold their commitment to universalism, they must not only ensure equal access to digital services but also protect citizens from exploitative data practices and opaque commercial entanglements. On the other hand, this raises critical questions about the agency and literacy of datafied publics (Kennedy et al., 2015). Are users who consent to tracking on municipal websites aware that they might be tracked by third parties? As studies demonstrate (e.g., Berens et al., 2024; Götze et al., 2022), tracking can persist even when users decline cookies, revealing the limits of consent as a meaningful expression of agency. Moreover, does trust in the state lead users to accept cookies on public service platforms, assuming – perhaps incorrectly – that these services do not engage in commercial tracking?

Future research should raise this issue with citizens, especially bearing in mind that they are unlikely to be aware of the tracking (Utz et al., 2019) and, subsequently, that there is a cost in the first place. This supports the argument that consent frameworks do not guarantee meaningful choice but rather serve as regulatory compliance mechanisms that prioritise user compliance over genuine comprehension (Kennedy et al., 2021). Considering the question from a universalist perspective, however, it can be noted that universal principles align poorly with commercial motivations. When municipal websites effectively serve as advertising platforms for Alphabet and Meta, they embed themselves in commercial logics that ultimately serve to further strengthen these companies' market position. Notably, the municipalities themselves do not make any revenue from allowing trackers to harvest citizen data. Instead, they serve to monetise citizenship. While certain tracking functions may serve efficiency, feedback, and accessibility standards that align with the principle of universality, the vast majority of data extraction serves commercial purposes. Whether or not municipal websites would offer the same quality of service without user tracking remains a question for further research, but the subsidy issue should by no means be overlooked. Ultimately, these are two different kinds of costs, prompting questions as to the value of data privacy versus the burden of taxation potentially incurred by rendering digital welfare state infrastructures wholly public.

Conclusions

The main contribution of this study is a detailed mapping of third-party trackers of previously unexplored municipal websites in a welfare state context. By doing this, the study sheds light on how local public welfare and global commercial platform companies are connected through digital infrastructure. This digital infrastructure is simultaneously omnipresent and virtually invisible. It is invisible to citizens because the only way this infrastructure is made apparent to them (if at all) is through reductionist consent buttons that may or may not stop them from being surveilled. Furthermore, these infrastructures of datafication are largely invisible in media and communication research, as trackers are not a common object of study. Thus, as two additional contributions, the study first highlights that trackers are conceptually important objects of study and, second, demonstrates a novel methodological approach as to how the connections between governmental bodies and tech platforms can be researched empirically, thus illuminating the growing data welfare society.

More specifically, the study has shown that digital government portals in Scandinavia are replete with commercial trackers, dominated by Alphabet and Meta. The data collection facilitated by this digital infrastructure constitutes an indirect, hidden cost on the user, amounting to a dual payment whereby citizens 1) subsidise government services with their personal data, and 2) fuel the analytics of advertising. The profiling potential that municipal portals render is almost unprecedented in the digital domain, as use of these sites provide data that infer citizens' civil and employment status, family situation, property holdings, and mobility. Hence, while the first cost might conform with shifts towards privatisation of the welfare state, the second constitutes a commercialisation of public spaces, blurring the line between citizen and consumer. Scandinavian governments should therefore realise that their websites constitute welfare state infrastructure, and second, regulate these spaces according to universal principles to ensure a fair, decommodified data welfare state (Andreassen et al., 2021). In practice, this would mean mobilising the two kinds of costs derived from this analysis to separate data-as-subsidy from its commercial use, and remove advertising functions from municipal websites. Furthermore, we recommend that municipalities remove analytical trackers from their websites, ban Google Analytics to ensure compliance with GDPR, and switch to open-source technologies to strengthen the universality of digital government infrastructure in Scandinavia. Finally, a fair data welfare state would also include (analogue) solutions for citizens who do not want to be digitally included.

Further research on trackers should explore and compare their technical evolution, prevalence, and functionality, not only cross-country but also across diverse public service ecosystems, for example, municipality, healthcare, government, and public service media websites. Research should also focus on emerging tracking technologies that bypass traditional trackers, such as fingerprinting. Moreover, there is a need to vet the regulatory landscapes across welfare states and assess how data privacy protections could be reinforced

to align with universal principles. Future work could also look at the way public policy goals toward increased digitisation have facilitated the adoption of commercial tracking, both directly and indirectly. As governing bodies continue to digitalise services, research should also investigate noncommercial, open-source solutions to replace the functions currently provided by commercial trackers, thereby enhancing data sovereignty and transparency.

In conclusion, while the digitalisation of public services can foster accessibility and efficiency, it should not compromise the welfare state's foundational principles. Aligning digital governance with privacy safeguards and ensuring transparency in data use are essential steps for maintaining citizen trust and preserving the public character of these services.

Limitations

While this study provides a comprehensive analysis of trackers on Scandinavian municipal websites, it has certain limitations. First, our research primarily focuses on tracking mechanisms visible through web archives, potentially overlooking more advanced tracking techniques, such as fingerprinting or cross-device tracking, which could further impact citizens' privacy. Another limitation is the study's scope, which does not include the user experience or perceptions of tracking on public service offerings, meaning that the extent of awareness and attitudes towards data-as-payment remains an open question. Lastly, while we identify tracking across different time periods, we do not investigate whether third-party trackers remain active even when users decline consent, a critical aspect given the limitations of GDPR compliance. Future research should address these gaps by integrating qualitative approaches, technical auditing of tracking persistence, and cross-national comparison of regulatory effectiveness.

Acknowledgements

This research is funded by the Research Council of Norway (grant number 314257) and the Swedish Research Council (grant number 2022-05392).

References

- Andreassen, R., Kaun, A., & Nikunen, K. (2021). Fostering the data welfare state: A Nordic perspective on datafication. *Nordicom Review*, 42(2), 207–223. <https://doi.org/10.2478/nor-2021-0051>
- Andrejevic, M. (2013). Exploitation in the data mine. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of web 2.0 and social media* (pp. 71–88). Routledge. <https://doi.org/10.4324/9780203806432>
- Andrews, L. (2019). Public administration, public leadership and the construction of public value in the age of the algorithm and 'big data'. *Public Administration*, 97(2), 296–310. <https://doi.org/10.1111/padm.12534>
- Baltz, A. A. (2020). A longitudinal analysis of Swedish local governments on Facebook: A visualisation of communication. *Nordicom Review*, 41(2), 147–162. <https://doi.org/10.2478/nor-2020-0020>
- Barassi, V. (2019). Datafied citizens in the age of coerced digital participation. *Sociological Research Online*, 24(3), 414–429. <https://doi.org/10.1177/1360780419857734>

- Barker, D. (2016). *Web content management: Systems, features, and best practices*. O'Reilly Media.
- Berens, B. M., Bohlender, M., Dietmann, H., Krisam, C., Kulyk, O., & Volkamer, M. (2024). Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security*, 136, 103507. <https://doi.org/10.1016/j.cose.2023.102507>
- Broomfield, H., & Reutter, L. (2022). In search of the citizen in the datafication of public administration. *Big Data & Society*, 9(1), 1–14. <https://doi.org/10.1177/20539517221089302>
- Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498–512. <https://doi.org/10.1145/42411.42413>
- Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction: Platforms and infrastructures in the digital age. *Information Systems Research*, 29(2), 381–400. <http://doi.org/10.1287/isre.2018.0794>
- Coyle, D. (2018). Platform dominance: The shortcomings of antitrust policy. In M. Morre, & D. Tambini (Eds.), *Digital dominance: The power of Google, Amazon, Facebook and Apple* (pp. 50–70). Oxford University Press.
- Elvy, S. A. (2017). Paying for privacy and the personal data economy. *Columbia Law Review*, 117(6), 1369–1459.
- Esping-Andersen, G. (1990). *The three worlds of welfare capitalism*. Polity.
- European Union. (2016). Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. *Official Journal of the European Union*, L327/1. <http://data.europa.eu/eli/dir/2016/2102/oj>
- Fehrenbach, D., & Herrando, C. (2021). The effect of customer-perceived value when paying for a product with personal data: A real-life experimental study. *Journal of Business Research*, 137, 222–232. <https://doi.org/10.1016/j.jbusres.2021.08.029>
- Flensburg, S., & Lomborg, S. (2023). Datafication research: Mapping the field for a future agenda. *New Media & Society*, 25(6), 1451–1469. <https://doi.org/10.1177/14614448211046616>
- Flyverbom, M. (2017). Datafication, transparency and trust in the digital domain. In European Commission: Directorate-General for Research and Innovation, *Trust at risk: Implications for EU policies and institutions* (pp. 69–84). Publications Office of the European Union. <https://doi.org/10.2777/364327>
- Fourcade, M., & Gordon, J. (2020). Learning like a state: Statecraft in the digital age. *Journal of Law and Political Economy*, 1(1), 78–108. <https://doi.org/10.5070/LP61150258>
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderators, and the hidden decisions that shape social media*. Yale University Press.
- Götze, M., Matic, S., Iordanou, C., Smaragdakis, G., & Laoutaris, N. (2022, June). Measuring web cookies in governmental websites. *Proceedings of the 14th ACM Web Science Conference 2022*, 44–54. <https://doi.org/10.1145/3501247.3531545>
- Helles, R., Lomborg, S., & Lai, S. S. (2020). Infrastructures of tracking: Mapping the ecology of third-party services across top sites in the EU. *New Media & Society*, 22(11), 1957–1975. <https://doi.org/10.1177/1461444820932868>
- Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society*. John Wiley & Sons.
- Hjelholt, M. F. (2024). The absorbent digital welfare state: Silencing dissent, steering progress. *Journal of Sociology*, 60(3), 643–659. <https://doi.org/10.1177/14407833241253632>
- Hokka, J. (2022) Welfare data society? Critical evaluation of the possibilities of developing data infrastructure literacy from user data workshops to public service media. In A. Hepp, J. Jarke, & L. Kramp (Eds.), *New perspectives in critical data studies: The ambivalence of data power* (pp. 267–294). Palgrave MacMillan. https://doi.org/10.1007/978-3-030-96180-0_12
- Hu, X., & Sastry, N. (2019, June). Characterising third party cookie usage in the EU after GDPR. *Proceedings of the 10th ACM Conference on Web Science*, 137–141. <https://doi.org/10.1145/3292522.3326039>
- Jakobsson, P., Lindell, J., & Stiernstedt, F. (Eds.). (2024). *The future of the Nordic media model: A digital media welfare state?* Nordicom, University of Gothenburg. <http://doi.org/10.48335/9789188855893>
- Jørgensen, R. F. (2024). Digital welfare – From the perspective of Nordic values and rights. *Nordisk Vælfærdsforskning | Nordic Welfare Research*, 9(2), 193–198. <https://doi.org/10.18261/nwr.9.2.7>
- Kammer, A. (2016). A welfare perspective on Nordic media subsidies. *Journal of Media Business Studies*, 13(3), 140–152. <https://doi.org/10.1080/16522354.2016.1238272>

- Kaun, A., & Dencik, L. (2020). Datafication and the welfare state: An introduction. *Global Perspectives*, 1(1), 12912. <https://doi.org/10.1525/gp.2020.12912>
- Kaun, A., & Löfgren, H. (2024). From media welfare to data welfare. In P. Jakobsson, J. Lindell, & F. Stiernstedt (Eds.), *The future of the Nordic media model: A digital media welfare state?* (pp. 261–276). Nordicom, University of Gothenburg. <https://doi.org/10.48335/9789188855893-12>
- Kennedy, H., Poell, T., & Van Dijck, J. (2015). Data and agency. *Big Data & Society*, 2(2), 1–7. <https://doi.org/10.1177/2053951715611145>
- Kennedy, H., Steedman, R., & Jones, R. (2021). Approaching public perceptions of datafication through the lens of inequality: A case study in public service media. *Information, Communication & Society*, 24(12), 1745–1761. <https://doi.org/10.1080/1369118X.2020.1736122>
- Kildal, N., & Kuhnle, S. (2005). The Nordic welfare model and the idea of universalism. In N. Kildal, & S. Kuhnle (Eds.), *Normative foundations of the welfare state: The Nordic experience* (pp. 13–34). Routledge. <https://doi.org/10.4324/9780203695241>
- Kitchin, R. (2014). Big data, new epistemologies and paradigm shifts. *Big Data & Society*, 1(1). <https://doi.org/10.1177/2053951714528481>
- Libert, T., & Nielsen, R. (2018). *Third-party web content on EU news sites: Potential challenges and paths to privacy improvement* [Factsheet]. Reuters Institute for the Study of Journalism, University of Oxford. <https://doi.org/10.60625/risj-fr2x-ax36>
- Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.
- Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review*, 8(4), 1–10. <https://doi.org/10.14763/2019.4.1428>
- Mossberger, K. (2008). Toward digital citizenship: Addressing inequality in the information age. In A. Chadwick, & P. N. Howard (Eds.), *Routledge handbook of internet politics* (pp. 173–185). Routledge. <https://doi.org/10.4324/9780203962541>
- Ministry of Digitalisation and Public Governance. (2023–2024). *Prop. 93 LS: Law on electronic communication (ecom law)*. Ministry of Digitalisation and Public Governance. <https://www.regjeringen.no/no/dokumenter/prop.-93-ls-20232024/id3033688/>
- Pybus, J., & Coté, M. (2022). Did you give permission? Datafication in the mobile ecosystem. *Information, Communication & Society*, 25(11), 1650–1668. <https://doi.org/10.1080/1369118x.2021.1877771>
- Ranchordas, S., & Scarcella, L. (2021). Automated government for vulnerable citizens: Intermediating rights. *William & Mary Bill of Rights Journal*, 30(2), 373–418. <https://scholarship.law.wm.edu/wmborj/vol30/iss2/8>
- Redden, J. (2018). Democratic governance in an age of datafication: Lessons from mapping government discourses and practices. *Big Data & Society*, 5(2). <https://doi.org/10.1177/2053951718809145>
- Rughiniş, R., Rughiniş, C., Vulpe, S. N., & Rosner, D. (2021). From social netizens to data citizens: Variations of GDPR awareness in 28 European countries. *Computer Law & Security Review*, 42, 105585. <https://doi.org/10.1016/j.clsr.2021.105585>
- Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, 6(1). <https://doi.org/10.1177/2053951718820549>
- Sanchez-Rola, I., Dell’Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P. A., & Santos, I. (2019). Can I opt out yet? GDPR and the global illusion of cookie control. *Proceedings of the 2019 ACM Asia conference on computer and communications security*, 340–351.
- Samarasinghe, N., & Mannan, M. (2019). Towards a global perspective on web tracking. *Computers & Security*, 87, 101569. <https://doi.org/10.1016/j.cose.2019.101569>
- Sjøvaag, H., & Ferrer-Conill, R. (2024a). Digital communications infrastructure and the principle of universality: Challenges for Nordic media welfare state jurisdictions. In P. Jakobsson, J. Lindell, & F. Stiernstedt (Eds.), *The future of the Nordic media model: A digital media welfare state?* (pp. 201–222). Nordicom, University of Gothenburg. <https://doi.org/10.48335/9789188855893-9>
- Sjøvaag, H., & Ferrer-Conill, R. (2024b). Working with datafication in media industries research. In U. Rohn, B. Von Rimscha, & T. Raats (Eds.), *The handbook of media economics* (pp. 93–104). DeGruyter. <https://doi.org/10.1515/9783110793444-007>
- Sjøvaag, H., Olsen, R. K., & Ferrer-Conill, R. (2024). Delivering content: Modular broadcasting technology and the role of content delivery networks. *Telecommunications Policy*, 48(4), 102738. <https://doi.org/10.1016/j.telpol.2024.102738>
- Sjøvaag, H., Stavelin, E., & Moe, H. (2016). Continuity and change in public service news online: A longitudinal analysis of the Norwegian Broadcasting Corporation. *Journalism Studies*, 17(8), 952–970. <https://doi.org/10.1080/1461670X.2015.1022204>

- Su, Z., Helles, R., Al-Laith, A., Veilahti, A., Saxena, A., & Simonsen, J. G. (2023). Privacy lost in online education: Analysis of web tracking evolution. In X. Yang, H. Suhartanto, G. Wang, B. Wang, J. Jiang, B. Li, H. Zhu, & N. Cui (Eds.), *Advanced data mining and applications* (pp. 440–455). Springer. https://doi.org/10.1007/978-3-031-46664-9_30
- Syvvertsen, T., Enli, G., Mjøs, O., & Moe, H. (2014). *The media welfare state: Nordic media in the digital era*. University of Michigan Press. <https://doi.org/10.3998/nmw.12367206.0001.001>
- Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 973–990. <https://doi.org/10.1145/3319535.3354212>
- van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- van Dijck, J. (2017). In data we trust? The implications of datafication for social monitoring. *MATRIZes*, 11(1), 39–59. <https://doi.org/10.11606/issn.1982-8160.v11i1p39-59>