General submission

EERJ European Educational Research Journal

European Educational Research Journal
1–20
© The Author(s) 2016
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/1474904116654917
eerj.sagepub.com
SAGE

Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education

Maria Lindh
The Swedish School of Library and Information Science, University of Borås, Sweden

Jan Nolin
The Swedish School of Library and Information Science, University of Borås, Sweden

Abstract

The aim of this study is to show how Google's business model is concealed within Google Apps for Education (GAFE) as well as how such a bundle is perceived within one educational organisation, consisting of approximately 30 schools. The study consists of two parts: 1) a rhetorical analysis of Google policy documents and 2) an interview study in a Swedish educational organisation. By making an implicit demarcation between the two concepts (your) 'data' and (collected) 'information' Google can disguise the presence of a business model for online marketing and, at the same time, simulate the practices and ethics of a free public service institution. This makes it problematic for Swedish schools to implement Google Apps for Education, bearing in mind Google's surveillance practices for making profits on pupil's algorithmic identities. From a front end viewpoint of Google Apps for Education, the advantages of the services are evident to the users, and emerge in the study, whereas back end strategies are relatively hidden.

Keywords

Cloud computing, algorithmic identities, Google Apps for Education (GAFE), privacy, surveillance economy

Introduction

This study focuses on digital surveillance in relation to public cloud services in Swedish schools. Today, an increasing number of both public and private schools, not only Swedish, are

Corresponding author:
Maria Lindh, The Swedish School of Library and Information Science, University of Borås, Sweden.
Email: maria.lindh@hb.se

implementing new forms of educational intermediaries (Williamson, 2015b) that serve to create a technological layer between and around pupils and teachers. The most highly touted of these is a Google cloud service specially made for schools – Google Apps for Education (GAFE). As GAFE is presented as a free to use service for schools, implementation seems to allow substantial savings in IT costs. In addition, with the implementation of GAFE, standards are supplied in all types of applications, which are, furthermore, easily convertible to each other. This means that schools struggling with the lack of common format standards (doc, pdf, odt, rtf, etc.) relating to digital communication between teachers and pupils are offered a solution. Taken together, Google seems to resolve both economic and practical issues.

Nonetheless, implementation has not been without controversy. In 2011, Salem announced that they were the first municipality in Sweden to implement GAFE. This prompted *the Swedish Data Inspection Board* to raise an injunction, arguing that pupils' privacy was threatened by its use. Despite unresolved policy issues regarding privacy, other educational organisations/municipalities in Sweden have followed in Salem's wake. Since 2011, agreements with Google have been signed in many Swedish municipalities as well as with individual school organisations.

How GAFE is perceived in schools is of importance for the coming development of information and communication technologies (ICTs) in schools, not only in Sweden, but also worldwide. Keen (2015) noted that idealists, overtly scorning commercial usage, originally created internet-based technologies as a public good. However, during the last two decades, internet has become colonised by a few multinational private sector actors. Google holds considerable power over internet usage through their different services – such as Google Search, Google Maps, Google Earth, YouTube, Google Translate, Google Books, Google Scholar, etc. Google is one of the four giant multinational corporations that claim ownership of most about everything digital in modern life, often referred to as GAFA (Google, Apple, Facebook, Amazon) (cf. Barraux, 2013). Given that this power structure also extends to smart phones and tablet computers, through the Android operating system, we find the trend to implement GAFE in schools somewhat problematic in at least two ways. First, we see the development of what Williamson (2015a, 2015b) labels 'digital education governance' in which educators and pupils become reconfigured as targets for data mining, tracking and measurement. This also involves shifting focus from the classroom to the algorithmic identity of the 'data double'. Second, the publicly funded compulsory school system in countries such as Sweden seems to be fraternising with opaque business interests. In a book co-authored by former Google CEO Eric Schmidt, the power involved is made explicit:

> We believe that the modern technology platforms, such as Google, Facebook, Amazon and Apple, are even more powerful than most people realize, and our future world will be profoundly altered by their adoption and successfulness in societies everywhere. These platforms constitute a true paradigm shift, akin to the invention of television, and what gives them their power is their ability to grow – specifically, the speed at which they scale. Almost nothing short of a biological virus can spread as quickly, efficiently or aggressively as these technology platforms, and this makes the people who build, control and use them powerful too. (Schmidt and Cohen, 2013: 9–10)

Judging by this statement, it would seem those implementing technologies of digital education governance such as GAFE are likely to miss the mark when estimating the impact of 'going with Google'. Such attempts are further hampered if corporations, such as Google, mislead school organisations regarding the business model involved. In this study, we therefore initially focus on how Google in policy documents creates distance from involvement in a kind of 'surveillance economy'. Thereafter, we turn to perceptions of GAFE and surveillance in the context of implementation within a Swedish school organisation.

After the literature review, we will briefly sketch a background to the introduction of commercial interests and educational information technology into the public school system. Following this, we will introduce the business model of web 2.0 corporations, particularly Google. In doing so, we describe two vital distinctions: *front end*/*back end* and the *processor*/the *archive*. This sets the scene for the two interlinked parts of the study. The first is devoted to a business model embedded within a 'surveillance economy', as it is portrayed in user oriented policy documents, i.e. mediation of inscribed policy concepts such as *data* and *information*. Our interest is how Google uses these concepts rhetorically. We thereby attempt to uncover what is actually done with pupils' data/information. Google policies, we argue, are written with the intention of concealing the business model. The second part concerns perceptions of GAFE as it was implemented within one Swedish educational organisation, consisting of approximately 30 schools. The purpose of combining these two parts is to uncover the gap between perceptions of GAFE within education – front end – and Google's expropriate use of pupils' data/information – back end. The paper concludes with a discussion and conclusion.

Literature review

The study at hand is inspired by several approaches. Building on *Science and Technology Studies* (STS), we view GAFE as a socio-technological constructed artefact inscribed with implicit social values (e.g. Fuller and Collier, 2004; Johansson, 1997; Toscano, 2012). STS is mostly concerned with the social dimensions of technological innovation, much less with the impact that technology has on social structures. Such a focus has been developed within *Software Studies*, acknowledging the power of code/software in society (e.g. Berry, 2011; Manovich, 2013). Most pertinent for the current study, ICTs, software, code, algorithms and data within the *educational sphere* have been critically scrutinised within this research approach (e.g. Edwards, 2015; Edwards and Carmichael, 2012; Lynch, 2015a, 2015b; Williamson, 2015a, 2015b, 2016a, 2016b). Lynch stresses the importance in understanding the implications of software on policy and practice, while investigating the role of software in school reform (2015a) and the role of data in education (2015b). Edwards and Carmichael (2012) view code as actor, 'both enabling and constraining knowledge, reasoning, representation and students' (p.575). As actor, it has impact on education and is not a neutral tool (Edwards, 2015). This is in line with research, which is focused on 'digital governance' in public education in England (e.g. Selwyn, 2016; Souto-Otero and Beneito-Montagut, 2016; Williamson, 2016a, 2016b). In his studies on governing policy (2015a) and intermediary organisations (2015b) Williamson shows how the individual learner is 'constructed' by the analysis of data, based on web behaviour, where algorithms are used to predict individuals' future progress. In addition to STS and Software Studies, this study is also influenced by *Surveillance Studies*, an interdisciplinary research field that views algorithms as instruments of surveillance (e.g. Cheney-Lippold, 2011).

Earlier research about GAFE has mostly been explorations of educational opportunities (e.g. Brown and Hocutt, 2015; Railean, 2012;). In addition, there are plentiful of reports from professional educators, mostly emphasising practical/localised issues (e.g. Barlow and Lane, 2007; Klein et al., 2012; Scheid et al., 2012). There have been a few earlier studies with at critical perspective scrutinising GAFE as an instrument for digital surveillance (e.g. Roth, 2015; Weber, 2016).

Google Apps for Education – the service

GAFE consists of a suite of cloud-based application programs: Google Classroom (not in use by the school organisation studied at the time of data collection), Gmail, Google Drive, Google Calendar, Google Docs, Google Spread sheets, Google Presentation, Google Sites (only in use at a couple of schools at the time of the interviews) (Google for Education: Save time and stay connected, 2016). As of writing, Google claims to have 50 million students, teachers and administrators using GAFE (Google for Education: Tools schools can trust, 2016).

Schools, the Free Market and ICT

In recent decades, the idea of the ‘information society’ has greatly influenced the ICT trend in Swedish schools. This ‘may perhaps be driven more by economic than educational concerns’ (Player-Koro, 2012: 73) and has been hard to criticise, since both policy makers and researchers have created a ‘belief system’ that educational technology is ‘a potential force for positive change’ and can ‘solve pedagogical problems’ (Player-Koro, 2012: 70). In addition to the ‘information society’, the European Union and the OECD have been engaged in long-standing discussions on similar concepts such as the *information economy* (OECD, 1986), *learning economy* Lundvall and Johnson (1994) and, most importantly, the *knowledge-based economy* (OECD, 1996).

ICTs in education are pushed by IT vendors and can frequently be understood as a strategy for marketing new ICTs (Nivala, 2009; Robertson, 2003). Therefore, also the adaption of GAFE should be seen in the context of the evolving introduction of markets and choice reforms (Rönnberg, 2015) into public education. Le Grand and Bartlett (1993) aptly coined the concept ‘quasi-market’ (as opposed to ‘free market’) to describe a situation where governments retain a minimum of regulatory power and pupils become ‘customers’, using a free service. Ichilov (2012) has forcefully argued that the introduction of market terminology, discourse and practices translate into new epistemological positions that essentially transform all aspects of education. Governments, since the 1990s, have become increasingly pressured to transform public goods into private goods and, in addition, schools have continually been subjected to systematic cutbacks in public funding. This, in turn, has placed heavy demands on schools to continuously review and reduce all types of costs. The remaining dual ambition, of reducing spending and increasing efficiency, serves as a vital context for the introduction of GAFE.

GAFE and Google’s business model

It is important to bear in mind that GAFE services are usually free to utilise, since Google has a well-established business model that allows the creation of wealth through the processing of users’ behaviour on the web. Perhaps most crucially, Google’s information on users’ behaviour on the web is collected through the DoubleClick server and is thereafter packaged and sold to advertisers. In 2014 Google had revenues of 59 billion dollars from sales of advertisements (Google Inc., 2015). Following the perspective of Fuchs (2012, 2014) it can be argued that users are severely misled when they assume that Google supplies a free service. It is, in fact Google that has access to free digital labour, as people through their everyday practices produce the commodity that creates Google’s economic wealth. ‘Google’s exploitation of users is not only limited to its own sites, its surveillance process is networked, spreads and tries to reach all over the WWW’ (Fuchs, 2012: 46). Fuchs (2014) thus presents a view of humans as ‘instruments for economic accumulation’ (pp.279–280) in the advertising industry, where Google is one of several stakeholders. Fuchs (2012) argues that ‘Google is the ultimate economic surveillance machine and the ultimate user-exploitation machine’ (p.44), since they economically exploit all users’ data. Obviously, this threatens the individuals’ privacy (p.47).

Based on the background sketched above, we aim to show how Google’s business model is disguised in relation to the use of GAFE. This is executed by a rhetorical analysis of Google policy documents and an interview study in a Swedish educational organisation, where perceptions of privacy are studied in relation to GAFE.

Google's business model – front end/back end

In short, the business model Google uses involves *front end* – free services – and *back end* – information packaged for profit (van Dijck, 2013). Considering the front end of GAFE, the services' advantages are evident to the users, whereas back end strategies are relatively hidden. As is shown in this paper's rhetorical analysis, the corporate strategy, according to Google policy documents, is to analyse users' information behaviour on the web to create tailored information for use in advertising. Arguably, with increased Google lock-in, more precise, individually customised information can be produced.

As Gehl (2014) has pointed out, computers are ruled by a sociotechnical dichotomy of tremendous importance: the *processor* and the *archive*. This distinction has been further played out as web 2.0 corporations have emerged. Front end activities are basically concerned with what the processor can do. However, web 2.0 corporations (of which Google is the most iconic) build on an original idea of giving away processing for free while retaining ownership of the archive. Gehl (2014) argues that we are dealing with two different kinds of logics, that of the immediate now (front end/processor) and the archived past (back end). While users are creating content in the present, the owners of the applications 'command the past, a past largely imagined to be an increasingly granular map of user desires' (Gehl, 2014: 48). As an ideological principle, web 2.0 applications tend to be designed with an emphasis on 'processors' which seduces users into what is happening right now. As noted by Gerben (2009), newness is privileged 'as a default design principle'. This emphatic push for new content will continuously feed and develop the archive.

An important part of this web 2.0 business model is to have exclusive ownership of a specific user generated archive. However, in their policy documents Google sometimes implies that it does not aspire to any such monopoly. For instance, Google states on its homepage that its *mission* 'is to organise the world's information and make it universally accessible and useful' (Google, 2016). This is no mean feat. The 'world's information' signals access to all archives, not only data produced on Google platforms. The act of creating universal accessibility would, of course, defy the business model of any web 2.0 corporation.

For decades, it has been of vital interest for corporations to acquire as much information as possible about customers, or potential customers. According to Turow (2011) the advertising industry now uses different tactics on the web to collect and analyse information about individuals in ways previously not possible. There are now far more sophisticated tactics for finding out more about customers, thereby attaining better control over the future of businesses. Today tactics – such as cookies and anonymous identifiers – have been refined, using digital information connected to individual users, called *personalisation*, *customisation* or *tailoring*. Cheney-Lippold (2011), among others, has identified patterns in which personal behaviour, surfing the web, is tracked to create *algorithmic identities* for online marketing. Algorithms are effective in filtering, sorting and prioritising information on the internet and have therefore been recognised as fundamental in getting access to knowledge and power in the hands of popular actors on the web. Beer (2009) states that there is an urgent need to understand how this power is played out, affecting the individual.

The processing of computer algorithms creates identities, which also are categorised based on the history of the user's online footprints (Cheney-Lippold, 2011). The 'algorithmic inference works as a mode of control, of processes of identification that structure and regulate our lives online within the context of online marketing and algorithmic categorisation' (p.164). These strategies are not at all dependent on the user's own data stored in a cloud, or on registered personal information, such as name, address, gender and age, which certain services require. Instead, surfing habits reveal the user and provide an algorithmic identity, which is continuously updated based on renewed algorithms.

Google policy rhetoric on exploitation of user data and information

The surveillance practice utilised by Google has been discussed in a wealth of texts (e.g. Andrejevic, 2007; Fuchs, 2011, 2012; Humphreys, 2011; Keen, 2015; Sullivan, 2014; Turow, 2011). However, many discussions fall short owing to the lack of transparency regarding Google's actual practices. It is easy to state that Google, as other web 2.0 corporations, creates wealth by utilising their exclusive access to a user-generated archive. Nonetheless, Google, as many other giants of the digital age frequently claim, 'we do not sell your data'. In the current section, we aim to make a contribution to this discussion through a rhetorical analysis of several Google policy documents. The purpose is to understand Google's rhetoric when explaining how they exploit the archive. Policy documents are, of course, crucial instruments in the creation of regulatory relationships between involved parties, i.e. manifestation of digital education governance. It is, therefore, problematic for all involved that such documents are frequently revised, combined or expanded in scope. Williamson (2015b) warns that contemporary educational intermediaries are to be seen as early examples of technologies that can be implemented in the years to come. Current policy documents need therefore to allow for future software, or to be continuously revised.

The starting point of our analytical work was the assumption that it would be fruitful to scrutinise Google policy documents as rhetorical texts rather than as guidelines. Policy texts are usually understood as neutral and informative descriptions of rules. This was, for instance, the character of the 26 social media policy documents analysed by Klang and Nolin (2011). However, these texts were aimed at standardising routines *within* an organisation. Policy texts aimed at customers may be written with other aims, balancing legal concerns with user readability. Such texts may become heavy with legal jargon and be difficult to understand and this was the case with the eight privacy policies analysed by Furnell and Phippen (2012). Our approach runs parallel in part to Turow's (2011), who examined Google's old privacy policy in 2011 and stated that 'the main theme of the privacy policy appears to be that Google protects 'personal information' while avoiding a central focus on advertising' (p.177). This impression is further reinforced by Edwards (2011) who previously worked for Google. He recalls a conversation between Google engineers and Google co-founder Larry Page:

> Well, some engineers asked, why don't we just tell people how we use cookie data to improve our products? … Larry opposed any path that would reveal our technological secrets or stir the privacy pot and endanger our ability to gather data … Users would oversimplify the issue with baseless fears and then refuse to let us collect their data. That would be a disaster for Google … (Edwards, 2011: 340)

Since technology developers such as Google are foremost into developing new technology, legal concerns are not within their scope. Schmidt and Cohen (2013) state: '… if Google stopped all product development whenever it found itself faced with a government suit, it would never build anything' (p.66). Instead, it seems Google trusts that legal concerns will be resolved once the technology is in place.

Building further on this assumption, we found it interesting to examine Google policy texts as rhetorical in character. When approaching a text from a rhetorical perspective, it is assumed that it has been designed to reach distinct goals of persuading specific audiences. Texts are therefore arranged in such an order that they maximise persuasion in relation to the goal. The aim of the rhetorical document is therefore markedly different than that of the purely informative policy document.

We aimed to collect and review all available and relevant policy documents provided by Google and not only those particularly concerned with GAFE. This is an important point of departure as Google services are intimately intertwined. As a result, we found that the GAFE webpage was directly linked to Google's privacy policy (Google for Education: Tools schools can trust, 2016). Indeed, Google famously unified 60 of 70 policy documents into one deliberately user-friendly privacy policy on 1 March 2012 (Google, 2012). In doing so, they argued that users would find the same rules and requirements for all Google services. Fairly consistent with Google's own account, we were able to identify six policy documents beyond the unified privacy policy document. In addition, we found it useful to review the vision articulated on Google's home page (Google, 2016). In the next stage of our process, we sought to identify the overarching aim of the rhetorical procedures in the different texts.

After having reviewed available policy documents, we suggest that the rhetorical aim of Google customer-oriented policy documents is to *disguise the business model* and to persuade the reader to understand Google as a free public service, divorced from marketplace contexts and concerns. We found it quite remarkable that the commercial aspects of Google's relationship to customers were so absent in the documents we reviewed. In fact, even though Google uses the term *customer* this may be something of a misnomer. A seller/customer relationship would seem to include some kind of financial exchange in return for goods or services, but here we understand the term customer as referring to non-paying users. Google tends to refer to their *paying customers* as 'third parties' or 'our partners'. Quite clearly, even the use of the 'customer' concept serves the strategy of making commercial practices invisible. At the next stage of our rhetorical analysis we therefore sought to identify further rhetorical tactics that were used to disguise the web 2.0 business model.

In order to carry legal weight, policy documents need to state that Google's constantly expanding archive is commercially exploited. However, the policy texts that we have reviewed are arranged in such a manner that this topic is separated from numerous other segments. This arrangement allows major parts of the policy texts to be worded as if Google does not have a web 2.0 business model or functions as a corporation within a marketplace. This is what we call a *procedural rhetoric*. Further, we have identified four separate rhetorical tactics that disguise the web 2.0 business model:

1. *Hands-off rhetoric*: Several segments of the policy texts state clearly, or so it seems, that the archive is not exploited, i.e. *we do not sell your data*.
2. *Benefiting rhetoric*: Exploitation of the archive is often framed as something that is primarily done in order to improve services for the user or the user experience. The commercial value is often not mentioned.
3. *Sidelining rhetoric*: Frequently, practices relating to the business model are belittled or framed as a minor aspect of what Google does.
4. *By example rhetoric*: Google is fond of explaining their practices through examples in their policy texts. In their privacy policy the phrase 'for example' is used 37 times (Google Privacy Policy, 2016). Frequently, practices can be explained both as front end (user service) and back end (business model) and in such cases, most examples only supply the former. From an epistemological viewpoint a wide range of examples can underpin knowledge claims. Different examples can always be chosen in order to emphasise or clarify a certain dimension of the knowledge claim. In order to explore a knowledge claim more fully, several examples need to be supplied. Google's systematic approach of giving one example connected to each claim is therefore misleading in more than one way.

The main rhetorical tactic is undoubtedly *hands-off*. This is often combined with *benefiting rhetoric*, Google claims that the user experience is more important than their 'own internal goal or bottom line' (Google, 2016). This is also expressed in Google's aim to be transparent:

> Whether it's real-time dashboards to verify systems performance, auditing of data handling processes or information about our data centers, we're committed to leading the industry in transparency. It's your data, and we want you to know what happens with it so that you always remain in control of it. (Transparency – Google for Work Help, 2016)

Google reassuringly claims that it is 'your data' and that you always have 'control of it'. This seems to imply that Google does not claim (exclusive) ownership of the archive and does not exploit it. On Google's webpages, information about trust and privacy is further specified, referring to how the user's data is processed. In their privacy policy it is stated that it is important to protect the customers' information:

> We do everything in our power to protect you and your businesses, schools, and government organisations from attempts to compromise your data. We vigorously resist any unlawful attempt to access our customers' data, whether it be from a hacker or a government body. (Privacy – Google for Work Help, 2016)

Here, we also find the *benefiting rhetoric*, with the claim that Google protects the data from being compromised by illegal access. An important part of this kind of rhetorical tactic is to expand on threats from external actors and, thereby, downplay problems involving Google itself. This tactic allows the development of certain segments of texts in which very little is said about how Google processes the data. Answering the questions: '*Is Google using my data? For what?*' they say that they do not sell their customers' data, they only process it:

> Google processes your data to fulfill our contractual obligation to deliver our services. Google's customers own their data, not Google. The data that companies, schools and students put into our systems is theirs. Google does not sell your data to third parties. Google offers our customers a detailed *Data Processing Amendment* that describes our commitment to protecting your data. (Privacy – Google for Work Help, 2016)

Once again, and here more emphatically, the *hands-off rhetoric* is utilised to claim that there is no exploitation of the archive in any way. There seems to be a loophole in the argument as Google alludes to processing of the data. Nonetheless, as far as we have seen, the key concept *processing* is not defined in the policy documents. It is reasonable to assume that this processing results in some kind of meta-data, for instance in the form of algorithmic identities. Still, some examples are given and are consistent with the *by example rhetoric* concerning front end services, implying that processing is about protecting users. Google states that it is 'scanning in Gmail' for GAFE, for 'virus and spam protection, spell check, relevant search results and features such as Priority Inbox and auto-detection of calendar events. Scanning to provide product features is done on all incoming emails and is 100% automated' (Google Apps for Education: Common Questions – Google Apps Administrator Help, 2016). Switching again to the *hands-off rhetoric*, they firmly state that they 'do NOT scan' GAFE emails with advertising in mind.

After analysing several Google policy documents it becomes obvious that the *hands-off rhetoric* is built around a crucial distinction between *data* and *information*. So, on the one hand, Google frequently refers to practices regarding 'your data' 'user data', 'personal data', 'customer data', etc. On the other hand, a completely different meaning is given to 'collected information', 'information that we collect' or 'information that you give us'. This distinction is never clarified as these concepts, although appearing frequently, are never defined. This is crucial as these concepts play a vital role in structuring the policy texts.

In order to understand Google policies, we need to render manifest the use of the terms *data* and *information*. Searching for definitions of what *data* refers to, we found only a definition of *personal data* as: 'submitted, stored, sent or received by Customer or End Users via the Services may include user IDs, email, documents, presentations, images, calendar entries, tasks and other electronic data' (Google Apps Data Processing Amendment, 2016). Obviously, this does not clarify if user data and personal data can be understood as equivalent.

Furthermore, *customer data* was defined as 'data (which may include personal data and the categories of data referred to in Appendix 1) submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users' (Google Apps Data Processing Amendment, 2016). These definitions referring to *data* serves as a foundation for the *hands-off rhetoric*. As long as Google is referring to 'data' they can emphatically state that 'you own your own data' and 'we do not sell your data'. Whenever the concept (your) 'data' is used, Google usually refers to numerous ethical principles of non-surveillance and non-commercial exploitation.

However, (collected) 'information' refers to something completely different than (your) 'data', namely the things that people do, i.e. their behaviour. In their privacy policy, Google lists at length 'information that we collect' including:

- personal information given to sign up services;
- device information (including hardware model operating system version, unique device and identifiers, mobile network and phone number);
- log information (including search queries, telephone log information, phone number, calling party number, time and date of calls, duration of calls, types of calls);
- IP address;
- device event information (including system activity, hardware settings, date/time of URLs visited, and browser type);
- identifying cookies;
- location information (including IP address, GPS and other sensor data);
- installed or uninstalled applications;
- local storage (including personal information);
- cookies and similar technologies.(Google Privacy Policy, 2016)

When utilising 'collected information', Google policy allows for a range of surveillance activities. In the *Privacy Policy – Privacy & Terms – Google* it is stated that 'personal information' is collected and this seems to refer to behaviour and networks. Instead of saying that Google collects information on the ads people click on and who they connect to on the web, the *benefiting rhetoric* is put into play and it is claimed that 'to provide better services' they are 'figuring out … which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like' (Google Privacy Policy, 2016). This is done through cookies and anonymous identifiers:

> We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google

> Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites. (Google Privacy Policy, 2016)

There is no clarification regarding who these partners are, but very few corporations worldwide can avoid having a relationship with Google. In the general privacy policy, it is clearly stated: 'Our automated systems analyse your content (including emails) to provide you with personally relevant product features, such as customised search results, tailored advertising and spam and malware detection' (Google, 2014). This is clearly a combination of *benefiting* and *sidelining rhetoric* also involving the curious phrase 'our automated systems', seemingly implying that living people are not in any way involved. It is a somewhat misleading turn of phrase since, obviously, numerous third-party corporations will have information about the individual preferences of users. Quite explicitly, emails, otherwise included in the *hands-off* 'user data' category, is included as a source for customised search results and tailored advertising, although Google states in their policies that they do not sell the data to 'third parties'. Referring to GAFE, Google states that they 'do not collect or use student data for advertising purposes or create advertising profiles' (Google for Education, 2016). They continue: 'Additionally, we do not collect or use any information stored in Apps for Education users' Google Drive or Docs (or Sheets, Slides, Drawings, Forms) for any advertising purposes' (Privacy – Google for Work Help, 2016).

There is obviously a dichotomy between (your) 'data' and (collected) 'information'. As this is not clarified, the privacy concerned user needs to be cautious. In the privacy policy, Google frankly states: 'When information is associated with your Google account, we treat it as personal information' (Google Privacy Policy, 2016). In another context, this would sound quite reassuring. However, as Google has declared an ambition to commercially exploit personal information, a more reassuring phrase in the current rhetorical context would instead be 'we treat it as personal data'. That said, 'personal information' is an interesting concept within the context of Google policy. It is, seemingly, situated between (your) 'data' and (collected) 'information' in a curious grey zone of its own. The concept itself is not defined although we are given some clues regarding 'sensitive personal information' which is characterised as something not registered: 'This is a particular category of personal information relating to confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality' (Google Privacy and Terms, 2016). Our interpretation is that 'personal information' as well as 'collected information' in these policy documents means *algorithmic identities*. It is then emphasised that 'sensitive personal information' is not used as a source in the construction of algorithmic identities, although it is not clear how this filtering is performed. When Google asserts 'we do not share personal information placed in our systems with third parties' (Google for Education: Tools schools can trust, 2016) it can be interpreted as: we do not sell our algorithmic identities of users. However, this does not mean that Google abstains from utilising these resources in order to produce targeted advertisement.

The privacy policy also supplies some relevant information on what Google does with collected information. Here, both *sidelining* and *benefiting rhetoric* tactics are utilised:

> We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads. (Google Privacy Policy, 2016)

This is, once again, an effort to rhetorically position this corporation as a non-profit organisation or a public service. The crucial 'also use', placed here as an afterthought, is really a statement regarding Google's business model.

Google is also explicit about the way that personal information is actively combined in order to counter users' attempts to develop multiple internet identities:

> We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. (Google Privacy Policy, 2016)

Naturally, it is economically advantageous to strengthen the algorithmic identity portrayed of individual users – the back end value. However, the *benefiting rhetoric* is utilised to portray this as a service rather than a vital economical driver.

In sum, then, Google makes an implicit demarcation concerning the archive through the two concepts (your) 'data' and (collected) 'information' and, thus, it becomes possible for Google to disguise the presence of a business model and to simulate the practices and ethics of a free public service institution. Judging by the policies it appears that Google elegantly divides the archive into two parts, rhetorically referring to one of them as hands-off. Thereby, it is implied that no economic exploitation of data/information connected to the user is involved at all. However, Google is also very clear about a wealth of tactics for tracking, archiving and exploiting user behaviour on the web.

Even though the implicit demarcation between data/information pursued by Google, to our knowledge, has not been recognised in earlier literature, it must be noted that monitoring behaviour has been emphasised in earlier literature. In his history of the development of social media Gehl (2014: 105) notes: 'As ad networks insinuated themselves into niche sites, marketers began to learn more about the desires of Web users. Surveillance of user activities has become the business model of online advertising'. Referring to Facebook, Google and Twitter, he continues: 'Their goal, from their earliest days, has been to produce audiences that adhere to tracking standards and deliver them to marketers' (p.106).

It is important to keep these tactics in mind as we later on move over to a specific case of GAFE within a Swedish educational organisation.

GAFE and legal difficulties

As Google has strived to standardise policies for all services, GAFE homepage provides a link to the general privacy policy. In addition, we find the main notions discussed above reiterated. At GAFE webpage this commonality is expressed as '[w]e are committed to protecting the privacy and security of all of our users, including students'. It is also stated that the service is *completely free* – 'Google Apps for Education is free for schools with 24/7 support at no cost. Never any ads, and your data is yours…' (Google for education: Save time and stay connected, 2016).

This statement not only emphasises the ubiquitous 'your data is yours' but also implies a completely non-commercial service with no disadvantages involved.

GAFE webpage provides several variations of this statement such as 'Google Apps for Education users own their data, not Google. The data that schools put into our systems is theirs, and we believe it should stay that way – it says so in our contracts' (Google Apps Terms of Service – Google Apps, 2016). It is furthermore stated that their 'commitment to the security and privacy of your data is absolute and we do everything in our power to protect you and your school from attempts to compromise it… Keeping your data safe is at the core of what we do… It's your data, and we want you to know what happens with it so that you always make informed choices' (Google Apps Terms of Service – Google Apps, 2016).

Nonetheless, it is not quite business as usual. In 2014 Google was hit with a federal legal suit regarding its practice of data mining student e-mails for purposes of targeted advertising (EPIC, 2014). Following this, in April 2014, Google announced the discontinuance of this practice, which, of course, concerned (your) 'data'. Furthermore, on the GAFE webpage (Google for Education: Tools schools can trust, 2016), Google announced signing of the *Student Privacy Pledge*, which was introduced by *The Future of Privacy Forum* and *The Software & Information Industry Association* to 'safeguard student privacy regarding the collection, maintenance, and use of student personal information' (Future of Privacy Forum and The Software and Information Industry Association, 2015). This page presents statements similar to Google policies. However, the vocabulary is slightly different. It is, for instance, stated that service providers should abstain from selling student information or performing behaviourally targeted advertising. However, 'selling student information' can be a matter of semantics and can be loftily interpreted as not 'selling algorithmic identities'. To abstain from tailored advertising would seem to be problematic for Google. Indeed, in December 2015 *the Electronic Freedom Foundation* filed a complaint with *the Federal Trade Commission* targeting this very issue connected to the pledge (Electronic Frontier Foundation, 2015).

Perceptions of Google Apps for Education

In the summer of 2014, interviews were conducted with strategic staff within management, education and IT in a Swedish educational organisation, consisting of approximately 30 schools, to investigate the respondents' perceptions of the implementation of GAFE, which occurred approximately one year before the interviews. The educational organisation had implemented GAFE, including tools such as Gmail, Google Drive, Google Calendar, Google Docs, Google Spreadsheets, Google Presentation, Google Sites and Google Chromebooks were also introduced to several student groups. The software and the device were integrated as a seamless solution to allow an optimal user experience of the free software.

Six face-to-face, semi-structured interviews were carried out in places chosen by the respondents. As these were involved in the implementation of many different individual schools, they can be seen as representatives of an evolving form of digital education governance. Given that implementation of GAFE was seen as successful, it seems reasonable to speculate that these actors will be involved in successive implementation of evolving technology in the years to come. The respondents' professional roles were: IT teacher (I1), IT director (I2), CIO (I3), director of education and development (I4), CMS-manager (I5), and former CEO (I6). The interviews, which were recorded, lasted between 90 and 150 minutes. All utterances connected to privacy were categorised into five themes: *legal regulations, security, access to data, surveillance* and *tracking identities*.

When the respondents discussed *legal regulations*, it became obvious that GAFE was perceived as problematic. Statements such as 'we noted that this is not legally tight' (I3), or 'we summarised by saying that 'the legal situation is unclear' in the management and the board' (I3). The organisation's previous ICT solution had created massive problems and caused a vulnerable situation for them. Therefore, on the board 'no one asked that much [about legal issues] since there were [ICT] problems to solve' (I3). Since the solution was perceived to be free of cost, some experienced that the board actually made a kind of non-decision – a kind of no-brainer. The former CEO expressed the situation:

> …we proposed that the costs [for ICT] would not increase. Party, huh. That's no problem! It's absolutely right! Or assume that [the costs] had increased by half a million every year and we came up with a suggestion that instantaneously would lower costs by one million. Yes, but then what? The next item on the agenda! These are decisions that make themselves. (I6)

According to the CIO, the organisation was prepared to take a risk since they 'saw how good the functionality between GAFE and Chromebooks was' (I3). Obviously there 'is of course a risk in using GAFE since the section paragraphs of *the Personal Data Act* do not hold' (I3). 'We said that we should take a chance and hope that the legal issues will be resolved' (I3).

> We manage almost everything with the new Google agreements from June 2014. The only thing we're not sure about is when a pupil erases data. Can Google then say that all that data is erased everywhere within seven days? They say that it takes thirty days, but you can't say that after thirty days everything is erased… (I3)

Privacy concerns were focused on what Google policy documents referred to as (your) 'data'. Data storage was seen as legally problematic for schools, since, perceptually there were uncertainties about how information is used by Google. Additionally, several respondents were worried about how to proceed if the educational organisation was forbidden to use GAFE in the future, owing to uncertainties related to *the Personal Data Act*, i.e. what information were to be regarded as sensitive: 'Certainly, there are uncertainties about what actually is sensitive information, or not. Therefore, you could probably find sensitive information in Google Apps or Gmail even if the staff has received directives' (I4, I5). The CIO had taken security measures to safeguard sensitive personal information from being handled in connection to GAFE. According to him, staff had been informed about how to handle sensitive information, i.e. not to handle it in GAFE. One respondent discussed the contradiction between principles and practice:

> Principally, you are not allowed to save information about pupils in GAFE. In practice, I have lists of pupils in my drive. I have had action plans for individual pupils lying around in my drive, which is not ok in principle. In practice, it is a storm in a teacup. Who in the world could find an action programme on my drive, where it says that a pupil has reading problems – and what difference does it make? As a matter of principle, it is in one way, but in everyday life… (I1)

This attitude to practice was not shared by the organisation, rather, GAFE was perceived *secure* enough for the type of information that should be handled in the system.

> You have to decide on an approach. What kind of information do I manage? I'm responsible for a school activity and that type of data … as I see it, when you work with the school system, like we do, I don't think there's any danger. I think that the information is sufficiently secure. (I3)

Another concern was that not only Google would have *access to data* (I3) and Google's files: 'You do not really have a document, only a link. If you were just cut off by Google, for some reason or another, then you haven't got a document any longer, but you take for granted that it works' (I5). This is a valid and practical concern. However, it is notable that the focus, again, is on what Google refers to as (your) 'data'.

Another theme was *surveillance*. The respondents recognised that GAFE carried an indirect non-economic cost, since payment was made with personal information (I1) and that Google could use this information for their own purposes (I3). Still, the Google business model, as articulated in policy documents, was not well understood as interview responses tended to be connected to cloud-based storage of 'your data' (according to Google terminology) while the more pressing privacy concern would be the way that Google monitors web, device and location-based behaviour. Therefore, one respondent articulated a fear that:

> If you are afraid of surveillance, then cloud services are not the most optimal. Then the information is not in your sphere any longer, but on some other server and there is a risk that they look into what you are doing. (I5)

On the other hand, some respondents felt that the information in systems such as GAFE was not that sensitive:

> There is no danger that information will fall into the wrong hands when you work with school systems [like GAFE]. Information on that level is not sensitive, it's secure enough. The worst that could happen is that incriminating information about individuals leak. (I3)

While the problematic dimensions of Google tracking user behaviour were not really recognised by respondents, it was interesting to find that the new technology allowed teachers to track pupil behaviour to a certain degree. For instance, the teachers could scrutinise the production of a document and follow how pupils proceeded with school tasks thus rendering learning processes more visible to teachers:

> You do not get a pile of examinations on the last day, but instead you follow their journey on their way. You can see what a pupil has written and then what another pupil has corrected. Or they have pasted a whole paragraph. 'From where does that paragraph come?' – You can conduct another type of discussion with the pupils. (I4)

This kind of surveillance of (collected) 'information' – using Google terminology – could be rather revealing. One respondent gave an example of a comment that could be communicated to the pupil: 'You created the document two days ago. We have had three weeks [to prepare for this task]' (I1).

In a follow-up question, it was queried if there also were problematic aspects involving the educational organisation's capacity to initiate surveillance over teachers' work. According to the CIO, 'That type of control organisation does not exist' (I3) and no such discussions among the teachers were known.

On the other hand, there were some concerns about monitoring user behaviour and this was articulated as a problem of pupils being identified. The CIO was worried about the legal issues involved in *tracking identities*. According to the CIO, it would be very difficult to decide what information could be defined as personal integrity data according to *the Personal Data Act*:

> When I have discussions with *The Swedish Data Inspection Board* [personal integrity data] seems to be everything … Pupils are not allowed to use own devices in school (such as iPads) because of the possibility to track their identities. They use their own iPhones, not primarily for schoolwork, but it is absolutely possible to do that.

It was reasoned that if pupils use personal devices, such as iPads or iPhones, Google will be able to identify users, since personal information is connected to their accounts. As a consequence, iPads were to be removed from schools. There were, therefore, some concerns about Google tracking identities:

> We have looked at using Google as an identity provider. We create the accounts there and they take care of them. It becomes smooth. But it's too big a security risk, and we will not own the account anymore, which we, of course, want to do. (I3)

Another solution to be implemented was to federate the different services into one account, created not by Google, but instead by the educational organisation itself:

> You can, in a way, say that a Google account is necessary for [a Chromebook] to work, but we are all in for GAFE, so we already have the account-problem … We have started to look into federation solutions, where the accounts are created by us. We will hold all account information, not Google. (I3)

As we can see from the result above, worries were foremost concerning the question of sensitive information – (your) 'data'. Identity tracking and personalisation – the outcome of knowledge about individual pupils' web behaviour, through cookies and anonymous identifiers – (collected) 'information' – was not recognised.

Discussion

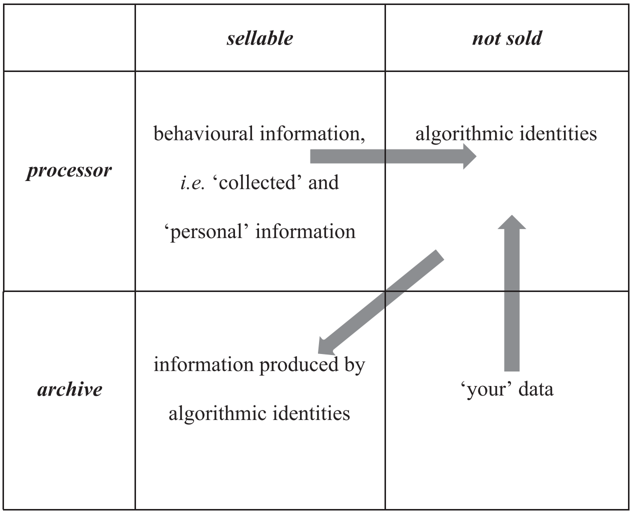
Keen (2015) claims that the free economy is being replaced by a surveillance economy and, as noted earlier, GAFE is thus a typical artefact of the surveillance economy. This can also be described in terms of the web 2.0 business model explained by O'Reilly (2009). Web 2.0 platforms provide services that are free for use while economic value is produced through the packaging of information generated at the proprietary platform. Basically, users are concerned with 'sharing' at the front end of the application while the platform owners are concerned with 'sharing' with third parties at the back end (O'Shaughnessy and Stadler, 2012; van Dijck, 2013). Sharing at the back end is seldom transparent to users, which also comes through in the interviews in our study.

What is then of value to Google when it supplies these free for use services? Google is deeply into the profiling of individual interests (Weitzner, 2007). On the one hand, this facilitates tailoring of search results. On the other hand, this feeds into the major business activity of helping corporations target their advertising. Fuchs (2012) characterises these practices as a blurring between producer and consumer, into a form of *prosumer* (concept originally coined by Toffler, 1980). In this way, Google becomes 'a meta-exploiter of all user-generated content producers' (Fuchs, 2012: 43). Granted, in the Swedish context, Google has committed itself only to saving pupils' data on a short-term basis. However, as is evident by their own policy documents, Google is less interested in exploiting this data and much more concerned with the monitoring of behaviour, i.e. to exploit the *collected* and *personal information*, creating algorithmic identities of individual users. As this is the case, most professionals engaged in implementing Google services will have difficulties in grasping the most pressing issues of the surveillance involved. Given the complexities we have constructed a tool in the form of a model (Figure 1) to be used by researchers and professionals in order to understand the legal position of Google, as it appears to us through their policy documents. We call this the *Back End Selling Model* as it is likely to be applicable to other platforms and corporations with the web 2.0 business model beyond Google.

Beyond the monitoring of behaviour – the 'collected' and 'personal' information – Google also has an interest in continuously processing *user data* in order to refine their algorithmic identities, which become valuable intellectual properties owned by Google to be utilised commercially but not sold to third parties. Judging by our reading of policy documents, this might be allowed for through the loophole of 'processing your data' even within GAFE. In addition, pupils will be using their Chromebooks in private as well. Consequently, all the substantial tools will be under the control of Google: hardware (Chromebook), system (Google Chrome web browser) and search engine (Google Search). Of course, Google can survey the performances of pupils using GAFE all over the world.

A further important commercial aspect, not addressed in the model (Figure 1), is that GAFE serves to accelerate routinised usage of a range of Google products. Not only is the Google brand considerably enhanced but there is also a potential of seducing young people all over the world into continuously choosing Google related products for various digital needs. This phenomenon has been discussed in terms of *vertically integrated chains* (Couldry and van Dijck, 2015), i.e. that internet giants such as Google and Facebook position themselves as gatekeepers of all internet activities.

GAFE is not only a powerful tool for Google. It can also be a dynamic tool for teachers. Teachers are already tasked with rating, ranking and ordering of pupils. Naturally, GAFE becomes a



	sellable	*not sold*
processor	behavioural information, *i.e.* 'collected' and 'personal' information	algorithmic identities
archive	information produced by algorithmic identities	'your' data

Figure 1. *The Back End Selling Model*, as constructed by the authors. The horizontal dimension show that the algorithmic identities are created from both the archive ('your' data), as well as from the processor (behavioural information), as the vertical and horizontal arrows show. Information/data from the algorithmic identities are further elaborated to fit third parties' interests (the diagonal arrow). The vertical dimension shows what information/data is sold, and not, by Google.

facilitator for these kinds of surveillance practices. It becomes much easier to overview, sort and compare pupils with this kind of technology. These affordances also suggest a renegotiation of the value of online versus offline performances. Online behaviour, documented and quantified through GAFE may easily be given more weight than classroom activities, since it supplies more distinct and quantifiable indicators of performance. Furthermore, not only pupils, but also teachers can now be evaluated by school leadership in ways earlier not possible, as their activities can be monitored, quantified and compared. It is interesting to see that perceptions in our interview study mainly concerned the legal and privacy aspects of using GAFE, whereas the surveillance aspects were given a lower profile. Although teachers themselves could practice surveillance of pupil behaviour, it was not perceived as an inherent Google standard practice.

In line with Williamson (2015b), GAFE can be characterised as 'governing software' similar to other recent applications such as Facebook for Educators, Make Things Do Stuff and Learning Futures. Such educational intermediaries serve to reconfigure what is seen as 'social' in terms of networked identities. Human actors, teachers and pupils alike, are understood as programmable socially networked creatures (Williamson, 2015b: 95). From a software studies perspective, software cannot be viewed as merely a technical tool but rather as something that codifies certain ways of thinking and acting.

To study Google's policy rhetoric is challenging, not owing to difficult terms but to the fact that central terms, such as *processing user data* or *content*, are not explained. Furthermore, different perspectives emerge in different documents, accomplished by hiding or leaving out important information. Therefore, it was highly motivated to study policies concerning GAFE and their other policies in relation to each other, rather than to look at each text separately. The result was contradictory; it is obvious that Google talks in different voices, deliberately wanting to make their business model less obvious for users, who mostly do not look deeply into Google's policies in any case.

Conclusion

Looking at the context of the Swedish school system, which has been compulsory and free of charge since 1842, the shift in successively involving the private sphere and promoting a surveillance economy is hazardous. We found it useful to build on Cheney-Lippold's (2011) ideas about how power is executed in society through knowledge about the citizens. Therefore, at stake is the pupils' algorithmic identity that can be utilised as a commodity by Google. By enticing evermore usage of Google services, users are given access to better and more efficient tools for processing their information needs. This, in turn, continuously develops the archive of 'collected' and 'personal' information that can be commercially exploited. In extension, this facilitates the attainment of societal, economic and political power.

Furthermore, GAFE involves another powerful technique, the programming not only of computer code but also of codes of conduct, imposed as uniform standards for schools all over the world. In this sense, the oft repeated warning of Lessig (1999, 2006) that 'code is law' is quite pertinent. Google retains control of code and can utilise the cloud-based character of GAFE to continuously change code with repercussions for practices in schools all over the world. It is seemingly easy to agree with Williamson (2015b: 101) in his argument that new forms of educational intermediaries 'contribute to emerging notions of learners as networked individuals whose 'social brains' are to be activated and optimised through new forms of software-mediated social learning'. Furthermore, GAFE and other contemporary applications seem to be quickly domesticated and normalised, thereby serving as the foundation for implementation of evolving technologies of big data, recommender systems and machine learning.

In the educational organisation studied in this paper, GAFE was perceived as a positive and well-functioning device, covering most of their ICT needs. Privacy issues were downplayed because of GAFE's advantages. The trend to implement ICTs in education is critical in this development, especially since it is considered to be steered by the IT industry, not from teachers' professional needs in education.

Furthermore, in the interview study most of the respondents did not bring up the subject of surveillance themselves, even though there were considerations when this issue was raised. As long as the federation solution could be pursued, the danger of insecure systems would be resolved. As privacy concerns, quite parallel to Google policy documents, were focused on *your data* rather than surveillance of behaviour – *collected* and *personal information*, critical discussions on implementations were aimed at a 'straw man'. The implicit decision to let Google use and sell pupils' information, enabling the creation of their algorithmic identities for advertising firms to exploit, was not addressed. This leads to a problematic situation. Pupils are left with no choice whether or not to use GAFE since school is compulsory and GAFE is the ICT in use. Can schools, or for that matter, municipalities, take responsibility for the exploitation of pupils' or employees' information? Why should the public school system force pupils to participate in the commodification of their digital labour and algorithmic identities?

The use of Google's cloud services in educational settings or other public organisations is arguably an issue requiring much further study given the rapid introduction of a powerful commercial application that furthers surveillance into public school systems and organisations all over the world.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Andrejevic M (2007) *iSpy: Surveillance and Power in the Interactive Era*. Kansas: University Press of Kansas.

Barlow K and Lane J (2007) Like technology from an advanced alien culture: Google apps for education at ASU. In: *Proceedings of the 35th Annual ACM SIGUCCS Fall Conference*, pp.8–10.

Barraux J (2013) Le drone et le tee-shirt. *Revue française de gestion* 5: 7–8.

Beer D (2009) Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media and Society* 11(6): 985–1002.

Berry D (2011) *The Philosophy of Software: Code and Mediation in the Digital Age*. Basingstoke: Palgrave Macmillan.

Brown ME and Hocutt DL (2015) Learning to use, useful for learning: a usability study of Google apps for education. *Journal of Usability Studies* 10(4): 160–181.

Cheney-Lippold J (2011) A new algorithmic identity: soft biopolitics and the modulation of control. *Theory, Culture and Society* 28(6): 164–181.

Couldry N and van Dijck J (2015) Researching social media as if the social mattered. *Social Media + Society*, 1(2): 1–7.

Edwards D (2011) *I'm Feeling Lucky: The Confessions of Google Employee Number 59*. London: Penguin Books Ltd.

Edwards R (2015) Software and the hidden curriculum of digital education. *Pedagogy, Culture and Society* 23(2): 265–279.

Edwards R and Carmichael P (2012) Secret codes: the hidden curriculum of semantic web technologies. *Discourse: Studies in the Cultural Politics of Education* 33(4): 575–590.

Electronic Frontier Foundation (2015) *Petitioner v. Google Inc: Respondent. Complaint and Request for Investigation, Injunction, and other Relief*. Available at: https://www.eff.org/files/2015/12/01/ftccomplaint-googleforeducation.pdf (accessed 1 February 2016).

EPIC (2014) *Google Admits to Data-Mining Student Emails*. Electronic Privacy Information Center. Published 19 March 2014. Available at: https://epic.org/2014/03/google-admits-to-data-mining-s.html (accessed 1 February 2016).

Fuchs C (2011) A contribution to the critique of the political economy of Google. *Fast Capitalism* 8(1): 1–24.

Fuchs C (2012) Google capitalism, tripleC: Communication, capitalism & critique. *Open Access Journal for a Global Sustainable Information Society* 10(1): 42–48.

Fuchs C (2014) Dallas Smythe reloaded: critical media and communication studies today. In: McGuigan L and V. Manzerolle V (eds) *The Audience Commodity in a Digital Age: Revisiting Critical Theory of Commercial Media*. New York, NY: Peter Lang Publishing, Inc., pp.267–288.

Fuller S and Collier JH (2004) *Philosophy Rhetoric and the End of Knowledge: A New Beginning for Science and Technology Studies*. London: Lawrence Erlbaum Associates, Inc., Publishers.

Furnell S and Phippen A (2012) Online privacy: a matter of policy? *Computer Fraud and Security* 2012(8): 12–18.

Future of Privacy Forum and The Software & Information Industry Association (2015) *About the Student Privacy Pledge*. Available at: https://studentprivacypledge.org/ (accessed 1 February 2016).

Gehl RW (2014) *Reverse Engineering Social Media: Software, Culture, and Political Economy in New Media Capitalism*. Philadelphia: Temple University Press.

Gerben C (2009) Privileging the 'New' in New Media Literacy: the future of democracy, economy, and identity in 21st-century texts, *Media in Transition 6*. Cambridge, MA. Available at: http://web.mit.edu/comm-forum/mit6/papers/Gerben.pdf (accessed 1 February 2016).

Google (2012) Official Google Blog: updating our privacy policies and terms, Posted: Tuesday, January 24, 2012. Available at: http://googleblog.blogspot.se/2012/01/updating-our-privacy-policies-and-terms.html (accessed 1 February 2016).

Google (2014) Google Terms of Service – Privacy & Terms – Google. Last modified: 30 April 2014. Available at: https://www.google.com/intl/en_uk/policies/terms/regional.html (accessed 1 February 2016).

Google (2016) About Google. Available at: https://www.google.se/intl/en/about/ (accessed 1 February 2016).

Google Apps Data Processing Amendment (2016) Version 1.5. Available at: https://www.google.com/intx/en/work/apps/terms/dpa_terms.html (accessed 1 February 2016).

Google Apps for Education: Common Questions – Google Apps Administrator Help (2016). Available at: https://support.google.com/a/answer/139019?hl=en (accessed 1 February 2016).

Google Apps Terms of Service – Google Apps (2016). Available at: http://www.google.com/apps/intl/en/terms/education_terms.html (accessed 1 February 2016).

Google for Education (2016). Available at: https://www.google.com/intl/nl/edu/privacy.html (accessed 1 February 2016).

Google for Education: Save time and stay connected (2016). Available at: https://www.google.com/intl/en/edu/products/productivity-tools/ (accessed 1 February 2016).

Google for Education: Tools schools can trust (2016). Available at: https://www.google.com/intl/en/edu/trust/index.html (accessed 1 February 2016).

Google Inc. (2015) 2014 Google Annual Report. Available at: http://www.annualreportowl.com/Google/2014/Annual%20Report (accessed 1 February 2016).

Google Privacy Policy (2016) Last modified: August 19, 2015. Available at: https://www.google.com/intl/en/policies/privacy/google_privacy_policy_en.pdf (accessed 1 February 2016)

Google Privacy & Terms (2016) Key terms. Available at: https://www.google.com/intl/en/policies/privacy/key-terms/ (accessed 1 February 2016).

Humphreys L (2011) Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication* 61(4): 575–595.

Ichilov O (2012) Privatization and commercialization of public education: consequences for citizenship and citizenship education, *The Urban Review* 44(2): 281–301.

Johansson M (1997) *Smart, fast and beautiful: On Rhetoric of Technology and Computing Discourse in Sweden 1955-1995*. Department of Technology and Social Change – Tema T. Linköping: Linköping Studies in Arts and Science, 245.

Keen A (2015) *The Internet is Not the Answer*. New York: Atlantic Monthly Press.

Klang M and Nolin J (2011) Disciplining social media: an analysis of social media policies in 26 Swedish municipalities. *First Monday* 16(8).

Klein R, Orelup R and Smith M. (2012) Google apps for education: Valparaiso University's migration experience. In: *Proceedings of the 40th Annual ACM SIGUCCS Conference on User Services*, pp.203–208.

Le Grand J and Bartlett W (1993) *Quasi-Markets and Social Policy*. London: Macmillan.

Lessig L (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lessig L (2006) *Code: Version 2.0*. New York: Basic Books.

Lundvall B-A and Johnson B (1994) The learning economy *Journal of Industry Studies* 1(2): 23–42.

Lynch TL (2015a) *The Hidden Role of Software in Educational Research: Policy to Practice*. London: Routledge.

Lynch TL (2015b) Mustard seeds and information feeds: a short history of students as data. *English Journal* 105(1): 96–98.

Manovich L (2013) *Software Takes Command: Extending The Language of New Media*. London: Bloomsbury Academic.

Nivala M (2009) Simple answers for complex problems: education and ICT in Finnish information society strategies. *Media, Culture & Society* 31(3): 433–448.

OECD (1996) *New Indicators for the Knowledge-Based Economy: Proposals for Future Work*. Paris: OECD.

OECD (1986) *Trends in the Information Economy*. Paris: OECD.

O'Reilly T (2009) *What is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*. O'Reilly Media Inc.

O'Shaughnessy M and Stadler J (2012) *Media and Society*. South Melbourne, VIC, Australia: Oxford University Press.

Player-Koro C (2012) *Reproducing Traditional Discourses of Teaching and Learning Mathematics: Studies of Mathematics and ICT in Teaching and Teacher Education*. Department of Applied Information Technology. Gothenburg: University of Gothenburg.

Privacy – Google for Work Help (2016) Trust. Available at: https://support.google.com/work/answer/6056650 (accessed 1 February 2016).

Railean E (2012) Google apps for education: a powerful solution for global scientific classrooms with learner centred environment, *International Journal of Computer Science Research and Application* 2(2): 19–27.

Robertson H-J (2003) Toward a theory of negativity: teacher education and information and communications technology. *Journal of Teacher Education* 54(4): 280–296.

Roth R (2015) The impacts on the educational landscape ahead the free internet offers, traps and surveillance that threatens the safety and privacy on the web. *International Journal of Learning, Teaching and Educational Research* 10(3): 102–127.

Rönnberg L (2015) Marketization on export: representations of the Swedish free school model in English media. *European Educational Research Journal* 14(6): 549–565.

Scheid EJ, Minato LH, de Oliveira Stein B, et al. (2012) Cloud computing with Google Apps for Education: an experience report. *Journal of Applied Computing Research* 2(2): 60–67.

Schmidt E and Cohen J (2013) *The New Digital Age: Reshaping the Future of People, Nations and Business*. London: John Murray.

Selwyn N.(2016) 'There's so much data': exploring the realities of data-based school governance. *European Educational Research Journal* 15(1): 54–68.

Souto-Otero M and Beneito-Montagut R (2016) From governing through data to governmentality through data: artefacts, strategies and the digital turn. *European Educational Research Journal* 15(1): 14–33.

Sullivan J (2014) Uncovering the Data Panopticon: the urgent need for critical scholarship in an era of corporate and government surveillance. *The Political Economy of Communication* 1(2). Available at: http://polecom.org/index.php/polecom/article/view/23/192 (accessed 1 February 2016).

Toffler A (1980) *The Third Wave*. London: Collins.

Toscano AA (2012) Analyzing technology to uncover social values, attitudes, and practices. *Marconi's Wireless and the Rhetoric of a New Technology*, Chapter 2. Dordrecht: Springer, pp.31–55.

Transparency – Google for Work Help (2016) Available at: https://support.google.com/work/answer/6056758?hl=en (accessed 1 February 2016).

Turow J (2011) *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth*. New Haven: Yale University Press.

van Dijck J (2013) *The Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press.

Weber AS (2016) The big student big data grab. *International Journal of Information and Education Technology* 6(1): 65–70.

Weitzner DJ (2007) Google, profiling, and privacy. *Internet Computing, IEEE* 11(6): 95–97.

Williamson B (2015a) Digital education governance: data visualization, predictive analytics, and 'real-time' policy instruments. *Journal of Education Policy* 1–19. Available at: http://dx.doi.org/10.1080/02680939.2015.1035758 (accessed 1 February 2016).

Williamson B (2015b) Governing software: networks, databases and algorithmic power in the digital governance of public education. *Learning, Media and Technology* 40(1): 83–105.

Williamson B (2016a) Digital education governance: an introduction. *European Educational Research Journal* 15(1): 3–13.

Williamson B (2016b) Digital methodologies of education governance: Pearson plc and the remediation of methods. *European Educational Research Journal* 15(1): 34–53.

Author biographies

Maria Lindh is a PhD student at the Swedish School of Library and Information Science, University of Borås, Sweden. Her general interest is information management and the current focus is on the complexity and co-construction of information technology within the organisational setting. The PhD thesis deals with the social shaping of cloud computing.

Jan Nolin is a professor at the Swedish School of Library and Information Science, University of Borås, Sweden. His background is within theory of science and his main research interest is the coproduction of internet technology and society.