Athens Journal of Education 2021, 9: 1-13
https://doi.org/10.30958/aje.X-Y-Z

Online Surveillance and Education for Digital Competence

By Lars Samuelsson[*] & Niclas Lindström[±]

Digital competence has become increasingly important in modern societies and is today central to the possibility of participating on equal terms as a citizen in a contemporary democracy. Thus, it is now stressed as a crucial learning objective, nationally as well as internationally. One pervasive consequence of the digitalization of society is the facilitation of intrusive online surveillance: when we are online, we leave traces that provide useful information to companies, organizations, and individuals, who can collect, process, use, and share this information. The purpose of this article is to reveal the need for an increased awareness of the surveillance aspect of digitalization in teacher education and schools. The argument is partly based on a questionnaire survey with 560 current and former Swedish student teachers, about online behavior and privacy. The results indicate that Swedish teachers in general need to further their digital competence in order to be able to appropriately aid their pupils in developing digital literacy. Given that Swedish student teachers can be expected to possess a comparatively very high level of digital competence, we think it is safe to generalize this point to comprise teachers in many other countries as well. We argue that an awareness of the surveillance aspect of digitalization is crucial to being a cognizant citizen in a democratic society, and that it should therefore constitute a natural part of education for digital competence.

Keywords: education for digital competence, digital competence, education for digital literacy, digital literacy, digitalization, online surveillance, soft surveillance, surveillance, surveillance culture, privacy

Introduction

Digital competence has become increasingly important in modern societies. Such competence is central to the possibility of participating on equal terms as a citizen in a contemporary democracy. Thus, it is nowadays stressed as a crucial learning objective, nationally as well as internationally. For example, it is one of the eight key competences for lifelong learning identified by The European Parliament and The Council of the European Union (European Union, 2006), and digitalization is one of the aspects covered by the UN sustainable development goal that concerns education (United Nations, 2021, SDG-4; see Indicator 4.a.1 and Target 4.b).

Navigating in a digital world requires competences such as the ability to find relevant information through search engines and databases, but also to practice criticism of the sources – consider, for instance, the current discussions about

[*]Associate Professor, Umeå University, Sweden.
[±]Associate Professor, Umeå University, Sweden.

misinformation and fake news. These competences – sometimes referred to as different aspects of *digital literacy* (American Library Association, 2021) – receive increasing attention in schools. However, digitalization comes with potential downsides, one of them being the facilitation of intrusive online surveillance. When we are online, we leave traces that provide useful information to companies, organizations, and individuals, who can harvest our data for various purposes.

While knowledge of this fact has become more widespread, it does not seem to get the attention that it arguably deserves in schools and teacher education. In Swedish teacher education, where we operate, surveillance issues in relation to online activities have not found a pronounced place in the curriculum. Yet, having knowledge in this area is important for making deliberate choices regarding one's online behavior – what information do I want to share, and with whom? For instance, is it worth giving away some of my personal information to get access to a certain social media platform?

There are some related issues regarding digitalization that do receive increasing attention in schools and teacher education (in Sweden as well as elsewhere): One concerns the risks of being more directly harmed in various ways in relation to the use of digital technologies – online bullying, or cyberbullying, is an important example of this (UNICEF, 2021), as are the risks involved in digitally sharing sensitive personal information or photos, and the risks of coming in contact with the wrong people (people with bad intentions) on the internet. Another issue concerns the high speed with which pictures and information can spread on the internet, the difficulty of removing them once they are out there, and the risk that they get distorted on their way through cyberspace. A third issue is that posting pictures on social media platforms may mean that you transfer legal rights to them to the companies running these platforms. These issues are all important, and it is a good thing that they receive more attention in schools and society at large. In this article, however, we are interested in the more subtle issue of online surveillance, which has not yet received as much attention in schools and teacher education, and whose effects are less direct or detectable:

Nowadays, data flow, largely unregulated, between different actors – companies, organizations, welfare institutions, private users, etc. These actors can take part of, and use, information about one another, for example via the digital traces that people leave when they use social media, do online shopping, search on Google, or use various games and other apps on their mobile devices. In addition, many of the online activities that are important to people require that they give away their data for others to collect, use, process, and share. For instance, when you sign up for Facebook, you agree to the following:

> We collect information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. […] We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners... (Facebook, 2021)

Other services use similar terms of agreement; terms that we rarely read, or, in case we do, typically comply with simply because we deem the services in question so important to us. Many people are unaware of the extent to which using such online services requires them to give away their data. We cannot expect young pupils – children – to acquire this awareness by themselves. And typically, we cannot expect their parents to have it either. Yet, as we will argue, such awareness is important to be able to make informed autonomous decisions regarding one's online behavior. At least to the extent that schools embrace digitalization, they arguably also have a responsibility to help pupils acquire such an awareness. (As we will elaborate below, this responsibility is plausibly also motivated by the democracy mission of school.) It is important to know what can and cannot be done to protect one's data. What risks, losses and gains are involved in various options? In the discussion section, we will return in more detail to why we think such an awareness is important, and why it is important that it is treated in school.

One key to acquire an autonomous and critical stance to one's own online behavior, is an understanding of how people generally behave in relation to privacy and sharing information online. Quite extensive research has shown that people tend to behave in ways that do not mirror their own privacy concerns. While they report strong concern for their privacy, they behave online as if their privacy were not very important to them at all. This has become known as the "privacy paradox": the "discrepancy between individuals' intentions to protect their own privacy and how they behave in the marketplace" (Norberg, Home, & Home, 2007, p. 101; for an overview, see, e.g., Kokolakis, 2017; Gerber, Gerber, & Volkamer 2018).

Within the framework of the research project "iAccept: Soft surveillance – between acceptance and resistance" (in which one of us is a participating researcher), a questionnaire survey was conducted with 560 current and former Swedish student teachers, about online behavior and privacy. At large, the responses are in line with the privacy paradox. Partly based on this survey, the present article aims to draw attention to the importance of raising awareness of the surveillance aspect of digitalization in teacher education and schools.

Purpose

The purpose of this article is to reveal the need for an increased awareness of the surveillance aspect of digitalization in teacher education and schools. We argue that an awareness of this aspect is crucial to being a cognizant citizen in a democratic society, and that it should therefore constitute a natural part of education for digital competence – or, differently put, that it should be seen as an important ingredient of digital literacy.

Outline

In the next section, we provide some background to our investigation: a brief account of surveillance and of the democracy mission of school. The subsequent section presents our method and research procedure and is followed by a

presentation of our findings. We end the article with a discussion partly based on these findings, followed by a short concluding remark.

Background

Surveillance – From State Surveillance to Surveillance Culture

Surveillance was long seen as a top-down affair, the typical case being that of a state surveilling its citizens. Indeed, for long the state was the only actor with the kind of resources and power required to practice large-scale surveillance, and arguably the only actor with an incentive to do so. The potential horrors of state surveillance were famously brought to public attention in George Orwell's novel *1984*, and in the seventies, Michel Foucault influentially revived the Benthamian notion of the panopticon, again putting the spotlight on top-down surveillance (see Foucault, 2009).

With the ongoing rapid digital transformation of society, this picture has changed dramatically. Nowadays, it is possible for anyone with access to a computer and the internet, and with sufficient knowledge, to surveil many other people to some extent. To describe the situation emerging from this development, David Lyon has coined the expression "surveillance culture", or "culture of surveillance", indicating that surveillance is something that we live in, that surrounds us, and that we have to relate to in one way or another:

> Once thought of mainly as the world of private investigators, police and security agencies, the means of surveillance now also flow freely through many media into the hands of the general public. This has helped to create an emerging surveillance culture – the everyday webs of social relations, including shared assumptions and behaviours, existing among all actors and agencies associated with surveillance. (Lyon, 2018, p. 30)

Rather than an exclusively top-down phenomenon, surveillance is here depicted as something more horizontal and reciprocal, where citizens also have the means to surveil each other. In addition, large companies and various organizations – political but also more shady ones (which – we have seen – may also be political (e.g., Colaresi, 2020)) – now have much to gain from collecting information about people in general. For instance, people (or small groups) can be individually and directly targeted with advertisements for various products, and with opinions wrapped in a way that suits the receiver (so called micro-targeting). As a more extreme example, people can get blackmailed as a result of their sensitive information ending up in the wrong hands.

Information – or data – has become a valuable currency. When we use for instance Facebook and Instagram, we do not pay with money, but with personal information (compare with Zuboff's (2019) notion of "surveillance capitalism"). It is easy to get the impression that the use of these platforms is free, but for most users it is not. All of us who use such platforms for personal communication, where

the whole purpose of using them would be undermined by anonymization, pay with valuable information that these companies can in turn trade for money with other companies who can use this information in various ways (see, for instance, the quote from Facebook above). We will return to this fact, and its significance for the present article, in the discussion section.

Another way in which the distinction between the earlier prevailing form of top-down surveillance, and the current forms of more horizontal surveillance, has been coined, is in terms of "hard surveillance" vs. "soft surveillance" (Marx, 2005) – the latter being the kind of online-surveillance (conducted primarily by commercial and noncommercial actors, such as businesses, NGOs, interest groups, researchers, political parties, and fellow citizens) that is based on us seemingly voluntarily giving away information through our usage of various products and platforms. However, the distinction is a fluid one, since governmental organizations can also make use of soft surveillance.

It is in light of the surveillance culture, and the practices of soft surveillance, that the current investigation takes place. We are interested in the awareness, or lack thereof, in educational contexts, of the consequences for ordinary people of living in the midst of the emerging culture of surveillance.

Democracy and Education

In this article we want to draw attention to the importance of possessing digital competence as an inhabitant of the culture of surveillance. Such competence, we will argue, is crucial to being a cognizant citizen in a modern democratic society, permeated by this culture. This is one main reason why this competence is something that should be furthered in schools. Apart from the fact that school is the place where we expect that our children get to learn about important societal matters, schools are nowadays generally considered to have a particular democracy mission – a special responsibility to foster democratic citizens, where this includes being competent in navigating within a democratic society.

Internationally, this aspect of education is stressed in, e.g., UNESCO's approach to Global Citizenship Education (GCED), including "[t]o acquire knowledge, understanding and critical thinking about global, regional, national and local issues and the interconnectedness and interdependency of different countries and populations" (UNESCO, 2015, p. 15). Arguably, this involves knowledge and understanding of the ongoing digitalization of society, the interconnectedness involved in it, and what it means to be a citizen of a digitalized society. The Council of Europe explicitly uses the term "Education for democratic citizenship", meaning:

> education, training, dissemination, information, practices and activities which aim, by equipping learners with knowledge, skills and understanding and moulding their attitudes and behaviour, to empower them to exercise and defend their democratic rights and responsibilities in society, to value diversity and to play an active part in democratic life, with a view to the promotion and protection of democracy and the rule of law. (Council of Europe, 2021)

In the Swedish curricula for the various school forms (from pre-school to upper secondary school) the democracy mission is very pronounced. For instance, the curriculum for the upper secondary school states that:

> It is not in itself sufficient that education imparts knowledge of fundamental democratic values. It must also be carried out using democratic working methods and develop the students' ability and willingness to take personal responsibility and participate actively in societal life. (Skolverket, 2013, p. 5)

This ability, we will argue, requires digital competence also regarding the surveillance aspect of the digitalization of society.

Method and Research Procedure

To a large extent, this is an argumentative article. It aims to draw attention to the importance of acknowledging the surveillance aspect of digitalization in educational contexts – with a particular focus on the democracy mission of school. However, it does so partly against the background of the results of a questionnaire survey that was distributed to various groups of current and former Swedish student teachers, at Umeå University, between November 2019 and May 2020. 560 current and former students answered the questionnaire, which contained various questions about online behavior and privacy, some of which are accounted for in the Findings section below. The study presented in this article is one of several part-studies of a larger project ("iAccept: Soft surveillance – between acceptance and resistance"). Hence, the questionnaire contained questions relevant to other part-studies as well, but here we only bring up the questions that are relevant to this part-study.

For the substantive questions in the questionnaire, we used an 11-point scale (ranging from 0 to 10), on which the respondents made their assessments or expressed their views (where 0 represented the lowest possible value and 10 the highest possible value, with 5 being in the middle). Presumably, such a scale allows fairly fine-grained assessments by the respondents without being too extensive. The survey was also aligned with previous studies in other European contexts, using partly similar questions and the same 11-point scale for assessments (see, e.g., Svenonius & Björklund, 2018; Sønderskov & Dinesen, 2016).

The current and former students who took part in the survey were invited to participate voluntarily under the condition that they could withdraw at any time. They were informed that their answers would be anonymized and treated as confidential. No personal data were stored. In this way, compliance to the general research ethical principles of informed consent, anonymity, confidentiality, and precautious use of collected information were ensured.

The survey was carried out through a web form distributed via the students' web-based learning platforms and in one case directly in the classroom. The invitation to participate in the survey was sent out to all students who entered teacher education at Umeå University between autumn 2012 and autumn 2019. This procedure gave us a low (and unknown) response rate, but a fairly high total

number of respondents. This suits the purpose of this study, in which we aim to track tendencies and reveal the need to raise awareness among teachers about certain aspects of digitalization, rather than to pursue statistical analysis. For this aim, a large number of responses – many representative voices – is more interesting than a high response rate. Even if the results of the survey would have looked somewhat different with a different selection procedure, what is important in relation to the points we want to make in this article is that so many student teachers answer the way they do.

Although we have a fairly high total number of responses, it is important to remember that we are considering the views of a limited number of current and former students from one university only, namely Umeå University in Sweden, and that the response rate is relatively low (as a result of how the survey was distributed). In other words, we are dealing with a so-called nonprobability sample (see Bryman, 2008, p. 183). In relation to this point we want to emphasize that the purpose of our investigation is not to draw precise conclusions about the percentage of Swedish student teachers holding certain views, but to track tendencies among this group and put them in relation to the issue we aim to draw attention to in this article. The results are not treated statistically, and we do not aim for a statistical analysis.

There are several reasons why we consider the surveyed group particularly interesting. One reason, of course, is that they plan to become teachers (some of them are already teachers). They are the ones who are supposed to help future pupils acquire digital competence, or digital literacy. And since they are not themselves likely to encounter the surveillance aspects of digital competence in teacher education to any significant degree (as noted above – this issue has not yet found a pronounced place in the curriculum for the Swedish teacher education), the views they express now are likely to be roughly the views they have when they meet their pupils. Secondly, this group is relatively well educated, as all of them are attending or have completed higher education, and they are familiar with computers, the internet, and social media; within the framework of their education, they have all been assigned to an online learning platform.

This background of our participants implies that – from a global and even a national perspective – they can be expected to possess a comparatively high degree of digital competence (even more so, probably, given our chosen selection procedure; it is likely that people who are interested in questions concerning various aspects of digitalization were more likely to choose to answer the questionnaire). Hence, if these respondents find various aspects of digitalization difficult or complicated, or if there are gaps in their digital competence, we should expect even more of this among people in general. Actually, in this respect Swedes in general constitute an interesting group in the present context, since the use of both the internet and social media is comparatively very high in Sweden (see DataReportal, 2020).

In the Findings section below, only a restricted number of the total findings from the survey are presented, namely those that are most relevant to the study

presented in this article. For a more comprehensive account of the survey and its results, see Cocq, Gelfgren, Samuelsson, and Enbom (2020).

Results

We begin by providing some background data from the survey to put the results we want to focus on in context. Of the 560 respondents, 70% report that they identify themselves as women (29% as men). As is to be expected given the group that was surveyed, the respondents are quite young: 66% are under 30 years old, and only 16% are over 40 years old. 39% report that they had a university degree of at least three years at the time of answering the questionnaire. 58% were studying and 38% were working. Their age and level of education further accentuate the point stressed above, that we can expect the members of this group to have a comparatively high level of digital competence.

Furthermore, the respondents report a high degree of social media usage. For instance, 82% state that they use Facebook at least a few times a week (65% claim to use it daily), and 89% state that they use Messenger at least a few times a week (69% claim to use it daily). However, they do not take measures to hide their data to any high degree. Only 21% report that they sometimes use a VPN service; 8% report that they use web browsers that do not store search results; and 36% report that they sometimes cover their computer camera. As many as 42% state that they sometimes use private mode in their web browser, but that privacy measure only conceals data locally.

At the same time – in line with the privacy paradox mentioned in the introduction – online privacy is important to most of the respondents (see Table 1). So, perhaps one should have expected them to be more cautious with their data. On the other hand, many respondents state that they find the issue of protecting their data complicated. Of the respondents who reported an opinion on the question of whether they think it is too complicated to care about the collection of their data, about half (267 out of 505 respondents, or 53%) responded more or less affirmatively (i.e., they marked some of the alternatives 5-10 on a scale from 0 to 10, where 10 was the most affirmative answer) (55 respondents did not report any opinion on this question) (see further Table 1). This may provide part of the explanation of the discrepancy between the respondents' reported behavior and their attitudes to their own online privacy.

Table 1. Views on Data Collection

To what extent do you agree with the following claims about data collection? [where 0 represents "not at all" and 10 represents "to 100 %"] The respondents had four claims to consider. For each claim, the table shows the percentage (rounded to the nearest integer) of respondents who marked the respective alternatives 0-10 and "no opinion"/"no answer" (-). (N=560)												
Claim	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**-**
It is important to me to be private/anonymous online.	1	1	4	6	7	21	9	14	14	7	13	2
I have nothing to hide, so I do not care.	10	3	6	8	7	19	7	10	13	6	6	4
It is too complicated to care.	15	5	9	6	7	14	9	9	8	3	4	10
I have good knowledge about how information about me is stored and transmitted when I use various services online.	8	9	11	14	9	11	8	10	9	4	3	2

Source: Survey conducted with student teachers at Umeå University, Sweden, between November 2019 and May 2020.

As Table 1 shows, the respondents do not generally consider themselves to have very good knowledge about how information about them is stored and transmitted when they use various services online – despite belonging to a group of which we can expect the members to have better knowledge about this than most people in the world. We will now discuss these results in some more detail in relation to digital competence, online surveillance, and the democracy mission of school.

Discussion

Our findings show that the student teachers we have surveyed largely display the familiar pattern which has come to be known as the privacy paradox (e.g., Gerber, Gerber, & Volkamer, 2018). They generally report that they care about their privacy, but at the same time they do not do much to protect that privacy when they are online. As noted above, our results indicate that one explanation of this (among our respondents) may be that many of them find the issue complicated and lack much knowledge about it. Yet, they are the ones who are supposed to help future pupils acquire digital competence. Now, why is this circumstance important? There are several reasons why we think it is, and here we want to highlight the ones that we initially have found most crucial.

Our general point is that an awareness of the "surveillance aspect" of digitalization is important to be able to make informed autonomous choices regarding one's online behavior. If we do not know that we are – or to what extent we are – being influenced and targeted for various purposes (based on the information that is continuously collected about us), we cannot consider if, and to what extent, we want to ward off this influence. This, in turn, risks to decrease our room for autonomous decision-making. Even if we are not aware of it, decisions may be – in a sense – partly made for us (namely, to the extent that the influencing

or targeting succeeds in altering our preferences or behavior, without our knowing or welcoming it). That is to say, we are not in full control of our own choices. Even if one believes that our opinions and choices are always a result of factors that lie outside of our control, it is usually thought to make a crucial difference, with respect to autonomy, whether we are aware of these factors and can consciously reflect on them and relate to them.

The potential lack of autonomy in decision-making may be considered particularly serious – from a democracy perspective – when the choices are of a political, evaluative, or ideological nature, i.e., when they concern our opinions on important matters (see Colaresi, 2020, for an extended discussion about digitalization and the threat to democracy).

There are several topical examples of large-scale political influencing and surveillance schemes utilizing digital technologies, the most well-known arguably being those associated with "the Snowden affair" (see, e.g., Burrough, Ellison, & Andrews, 2014) and "the Cambridge Analytica scandal" (the latter with connections to both the Trump 2016 election campaign and the pro-Brexit campaign; see, e.g., DCMS, 2018). By means of collected aggregated data, political (and other) actors can nowadays target specific groups iteratively with messages on a scale not seen before (e.g., Colaresi, 2020). Kenneth King explicitly addresses the issue of digital literacy and democracy in relation to Brexit, providing examples of such micro-targeted (mis)information aimed at specific groups in the UK (King, 2019). King draws on an investigation of disinformation conducted by the UK's cross-party Committee on Digital, Culture, Media and Sport (DCMS), which in its reports directly addresses the need for educational measures to tackle what is perceived as a huge democracy problem:

> In this rapidly changing digital world, our existing legal framework is no longer fit for purpose… We have highlighted significant concerns, following recent revelations regarding, in particular, political manipulation and set we out [sic!] areas where urgent action needs to be taken by the Government and other regulatory agencies to build resilience against misinformation and disinformation into our democratic system. Our democracy is at risk, and now is the time to act, to protect our shared values and the integrity of our democratic institutions. (DCMS, 2018, p. 3)

Based on its investigation, the DCMS committee concludes that "digital literacy should be the fourth pillar of education, alongside reading, writing and maths" (DCMS, 2018, p. 63; DCMS, 2019, p. 87).

In this article, we have aimed to emphasize the critical aspect of digital literacy that the DCMS committee (and King) draws attention to here. It is important to know and understand how one's data can be collected and used when being online – i.e., that it can be used by organizations and companies to expose one to tailored messages – as well as what can and cannot be done to protect one's data. What risks, losses and gains are involved in various options? As the examples of political micro-targeting and misinformation reveal, such knowledge is crucial to being a cognizant citizen in a modern democratic society. In light of the generally assumed

democracy mission of school, we contend that this aspect of digital literacy should therefore have a pronounced place in both schools and teacher education.

The results from our survey indicate that Swedish teachers in general need to further their digital competence in order to be able to appropriately aid their pupils in developing digital literacy. Given that Swedish student teachers can be expected to possess a comparatively very high level of digital competence, we think it is safe to generalize this point to comprise teachers in many other countries as well.

It is not only the political aspects of online surveillance discussed above that need to be considered in an educational context. Since the digital transformation of society also permeates its educational institutions, and more and more schoolwork is carried out using digital means, an awareness of the surveillance aspect of digitalization should be present in all schoolwork that makes use of online resources. For example, how many teachers reflect over the fact that when they ask pupils to search on Google, they simultaneously ask them to provide the company Google with information? It is easy to get the impression that platforms like Google are "just out there", completely free for us to use. But, as noted in the background section, that is not the case. To the contrary, these services are built on a business idea in which the basic commodity is our personal information (See Zuboff, 2019).

Perhaps most school assignments that require online activities are done on school computers (or other digital devices owned by the school), which may mitigate this kind of worry. However, there may be notable exceptions. During the ongoing pandemic, for instance, many pupils around the world have been educated online, from home, and perhaps used a personal computer with an IP address associated with themselves or their family. Even if the example of a school assignment requiring pupils to do Google searches from home may still be considered a rather innocent case, it illustrates the importance of knowing what one is doing when performing various online activities.

When pupils have been introduced to Google and other commercial online services in school, they will likely start to use them for purposes outside their educational sphere and begin to build their own personal data footprint for companies like Google to use and profit from. A person may be perfectly fine with this, and even regard it as something they want to be a part of – perhaps they like getting customized advertisements and do not see any considerably negative consequences for themselves of leaving digital footprints – but the point is that this should be an informed autonomous decision and not something that happens behind their back and outside of their control. Such control is something that schools should arguably help pupils to gain. For instance, perhaps teachers should provide their pupils with the possibility and knowledge of using a VPN-service when they ask them to do school tasks from home that require online activity. Be that as it may, the main point here is that awareness about these issues is still lacking to a large extent and yet it needs to be transmitted to the pupils.

One example of what can be done in teacher education to raise awareness of the surveillance aspect of digitalization, is to bring the privacy paradox to the students' attention and have them reflect on it. To become aware of this more or less unconscious, but to a large extent general behavioral pattern, may be a good

way to start the journey towards more conscious online behavior, which hopefully can lead to better preconditions for supporting one's future pupils in their development of digital literacy.

Conclusions

In this article we have discussed the need for raising awareness – in schools and teacher education – about the surveillance aspect of digitalization. We have done this against the background of survey results from former and current Swedish student teachers at Umeå University. We have argued that an awareness of this aspect is important to make autonomous informed decisions regarding one's online behavior, which in turn is crucial to being a cognizant citizen in a modern democratic society. Apart from the fact that school is the place where we expect that our children get to learn about important societal matters, the generally assumed democracy mission of school further accentuates the importance of making the surveillance aspect of digitalization a natural part of education for digital competence – or, differently put, to make sure that it is seen as a crucial ingredient of digital literacy. We hence want to encourage teachers in schools and teacher education to further educate themselves about these issues in order to be able to assist their pupils or students in developing this aspect of their digital competence.

Acknowledgments

This article was written as part of the project "iAccept: Soft Surveillance – Between Acceptance and Resistance" (MAW 2016.0092), funded by the Marcus and Amalia Wallenberg Foundation. We want to thank Coppélie Cocq, Jesper Enbom, and Stefan Gelfgren for valuable input.

References

American Library Association (2021). *Digital Literacy*. Retrieved from: https://literacy.ala.org/digital-literacy/. [Accessed 16 April 2021.]

Bryman, A. (2008). *Social Research Methods*. Oxford: Oxford University Press.

Burrough, B., Ellison, S., & Andrews, S. (2014, April 23). *The Snowden Saga: A Shadowland of Secrets and Light*. Vanity Fair. Retrieved from: https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview. [Accessed 19 April 2021.]

Cocq, C., Gelfgren, S., Samuelsson, L., & Enbom, J. (2020). Online Surveillance in a Swedish Context. *Nordicom Review, 41*(2), 179-193.

Colaresi, M. (2020). How our Misunderstanding of the Digital and Computing Revolutions Puts Democracy at Risk (and What to Do About it). *Critical Quarterly, 62*(1), 70-80.

Council of Europe (2021). *What is EDC/HRE*. Retrieved from: https://www.coe.int/en/web/edc/what-is-edc/hre. [Accessed 16 April 2021.]

DataReportal (2020). *Digital 2020: Global Digital Overview/Digital 2020: Sweden*. Retrieved from: https://datareportal.com/. [Accessed 16 April 2021.]

DCMS - Digital, Media, Culture and Sport Committee (2018, July 24). Disinformation and "Fake News": Interim Report. London: House of Commons.

DCMS - Digital, Media, Culture and Sport Committee (2019, February 14). Disinformation and "Fake News": Final Report. London: House of Commons.

European Union (2006, December 20). *Recommendation of the European Parliament and of the Council of 18 December 2006 on Key Competences for Lifelong Learning*. OJ L 394, 10-18. Retrieved from: https://eur-lex.europa.eu/eli/reco/2006/962/oj. [Accessed 13 April 2021.]

Facebook (2021). *Data Policy*. Retrieved from: https://www.facebook.com/about/privacy. [Accessed 15 April 2021.]

Foucault, M. (2009). *Security, Territory, Population: Lectures at the College De France, 1977-78*. London: Palgrave Macmillan.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security, 77*(Aug), 226-261.

King, K. (2019). Education, Digital Literacy and Democracy: The Case of Britain's Proposed 'Exit' from the European Union (Brexit). *Asia Pacific Education Review, 20*(1), 285-294.

Kokolakis, S. (2017). Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Computers & Security, 64*(Jan), 122-134.

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Marx, G. T. (2005). Soft Surveillance: Mandatory Voluntarism and the Collection of Personal Data. *Dissent, 52*(4), 36-43.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

Skolverket (2013). *Curriculum for the Upper Secondary School*. Retrieved from: https://www.skolverket.se/publikationsserier/styrdokument/2013/curriculum-for-the-upper-secondary-school?id=2975. [Accessed 16 April 2021.]

Svenonius, O., & Björklund F. (2018). Explaining Attitudes to Secret Surveillance in Post-Communist Societies. *East European Politics, 34*(2), 123-151.

Sønderskov, K. M., & Dinesen. P. T. (2016). Trusting the State, Trusting Each Other? The Effect of Institutional Trust on Social Trust. *Political Behavior, 38*(1), 179-202.

UNESCO (2015). *Global Citizenship Education: Topics and Learning Objectives*. Paris: United Nations Educational, Scientific and Cultural Organization.

UNICEF (2021). *Cyberbullying: What is it and How to Stop it*. Retrieved from: https://www.unicef.org/end-violence/how-to-stop-cyberbullying. [Accessed 13 April 2021.]

United Nations (2021). Goals: 4: Ensure Inclusive and Equitable Quality Education and Promote Lifelong Learning Opportunities for All. Retrieved from: https://sdgs.un.org/goals/goal4. [Accessed 13 April 2021.]

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.