INTERNET POLICY REVIEW
Journal on internet regulation

Volume 12 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

The transformation of surveillance in the digitalisation discourse of the OECD: a brief genealogy

Michaela Padden *Karlstad University*

DOI: https://doi.org/10.14763/2023.3.1720

Published: 8 August 2023
Received: 12 February 2023 **Accepted:** 12 May 2023

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Padden, M. (2023). The transformation of surveillance in the digitalisation discourse of the OECD: a brief genealogy. *Internet Policy Review*, *12*(3). https://doi.org/10.14763/2023.3.1720

Keywords: Profiling, Surveillance, Digitalisation, Organisation for Economic Co-operation and Development (OECD), Democracy

Abstract: In democratic states, mass surveillance is typically associated with totalitarianism. Surveillance practices more limited in their scope draw criticism for their potential to undermine democratic rights and freedoms and the functioning of representative democracies. Despite this, citizens living in political systems classed as democratic are increasingly subject to surveillance practices by both businesses and governments. This paper presents the results of a genealogy of OECD digitalisation discourse from the 1970s to the present to show how both harms and benefits of surveillance practices have been problematised. It shows how practices once considered unacceptable are increasingly portrayed as neutral, or even positive. A shift is identified from general agreement over the incompatibility of surveillance practices with democracy to greater acceptance of those practices when rebranded as tools to promote customisation, economic growth or public health. This transformation is significant because it: (1) shows the inherent instability of policies anchored to seemingly fixed or self-evident concepts such as 'well-being' or 'public interest'; (2) highlights the fragility of democratic systems when things deemed harmful to their operation can be repurposed and subsequently permitted; and (3) highlights the contingency of (seemingly inevitable) surveillance practices, thereby opening up a space in which to challenge them.

Introduction

Digitalisation is a *megatrend*, according to the Organisation for Economic Co-operation and Development (OECD), alongside globalisation, demographic change and climate change (OECD, 2019b, p. 4). Given the expansion in the use of surveillance technologies in ongoing digitalisation processes and the concern that surveillance practices may undermine democratic rights and freedoms, it is important to understand how surveillance is represented in digitalisation policy discourse. This paper takes the case of the OECD, whose role is to provide a forum for democratic countries with market-based economies and policy guidance on economic performance and international standard setting (OECD, n.d.). In 1980, the OECD produced the world's first internationally agreed guidelines on transborder data flows and privacy protection principles. This paper aims to identify how the concept of surveillance has been problematised in digitalisation discourse of the OECD from the 1970s to the present. By tracing representations of surveillance over time, it is possible to identify changes in how surveillance is understood, which will in turn produce lived effects. For example, mass surveillance practices such as the indiscriminate tracking of people's geographic locations, or the digital retention of educational records or health information (thus making it easier to share or be combined with other information to create profiles), shift from being represented as wholly unacceptable and incompatible with democratic forms of government to more acceptable when framed as tools to achieve customisation in public or private service delivery or more general 'public interest' goals such as public health or security. How surveillance practices are branded in policy discourse is important because their representation has social and political significance: surveillance understood as an instrument of totalitarianism versus surveillance understood as the key to a 'smart' future will help shape very different social and political realities.

Surveillance is a concept concerned with practices of "watching over", although the term itself has changed in meaning over time and remains contested (Lyon, 2022, p. 1). James Rule has defined surveillance as "the systematic collection and monitoring of personal data for the purpose of social control" (Rule et al., 1980, p. 90). David Lyon defines surveillance as "a social practice" concerned with "the focused, systematic and routine attention to personal details for the purposes of influence, management, protection or direction" (Lyon, 2022, p. 1; Lyon, 2007, p. 14). Importantly, the concept of surveillance has a political dimension, given its "associations with power and resistance" (Lyon, 2022, p. 1). "Mass surveillance" is defined as the indiscriminate monitoring of a population, or significant proportion of a population, regardless of whether the people being monitored are suspected of any

wrongdoing, either by governments or private corporations (Privacy International, 2021). "Dataveillance" (Clarke, 1988, p. 499) is "the systematic use of personal data systems in the investigation or monitoring of the actions of or communications of one or more persons". Whereas mass surveillance casts a wide, undiscriminating net, "targeted surveillance" is directed at specific individuals for whom prior suspicion has been established following procedures defined in law. Mass surveillance used by governments or state entities as an indiscriminate means of identifying wrongdoing has long been considered an instrument of totalitarianism (Watt, 2017). Yet, despite condemnation by European institutions of the indiscriminate monitoring of populations by governments as a threat to civil liberties, independent journalism and political opposition (European Parliament et al., 2015, p. 1; Council of Europe, 1950), large-scale and indiscriminate internet surveillance practices, such as the bulk collection of cross-border electronic communications by governments, have been legitimised in liberal states in the post-Snowden years (Tréguer, 2017). Tréguer refers to this "illiberal drift" as the "Snowden paradox", whereby illegal and "alegal" internet surveillance practices have been legitimised rather than shut down following Snowden's disclosures (Tréguer, 2017). This process has been reinforced by European Court of Human Rights (ECtHR) decisions in cases such as *Big Brother Watch v UK*, where it ruled that violations of Articles 8 (Respect for your private and family life) and 10 (Freedom of Expression) of the European Convention on Human Rights were due to a lack of procedural safeguards, rather than the legality of bulk interception and sharing regimes *per se* (Zalnieriute, 2021). Similarly, in both *Centrum för Rättvisa v Sweden* and *Weber and Saravia v Germany*, the ECtHR found a violation of Article 8 due to insufficient safeguards in bulk surveillance operations, rather than the illegality of bulk surveillance itself (Zalnieriute, 2021).

The term "surveillance practices" is used in this paper to denote large-scale data collection practices which are, or which could be, utilised for mass surveillance objectives as defined by Rule et al., Lyon and Clarke. Büchi et al. (2022, p. 1) provide a definition of dataveillance which captures the more indeterminate forms of monitoring about which this paper is concerned, being "the automated, continuous, and unspecific collection, retention, and unspecific analysis of digital traces by state and corporate actors". References to "surveillance practices" in this paper therefore include practices such as tracking, monitoring, data collection, retention, aggregation, correlation and profiling, but do not necessarily require the intention of social control which is present in the definitions of "mass surveillance" given by Rule and Lyon. Such surveillance practices are, however, the building blocks of mass surveillance architecture. As such, their representation in policy discourse is significant.

In order to identify "problem representations" of surveillance practices in OECD digitalisation policy discourse, the study adopts Carol Bacchi's (2009) "What's the Problem Represented to Be?" (WPR) approach, which examines policy solutions for their inherent "problem representations". If "terminology shapes reality" (Katzenbach & Bächle, 2019, p. 2) then the representation of surveillance practices in digitalisation policy is especially important given that it can reveal broader social trends, including the downplaying of previously articulated harms in favour of convenience or economies of scale. Awareness of discursive trends is important, especially at a time when much new EU regulation is being tested or drafted, such as the draft Artificial Intelligence Act (European Commission, 2021). This current moment of openness is also reflected in the legal uncertainty of certain surveillance technologies, such as facial recognition, or practices such as those used in targeted advertising. According to Giraudo (2021, p. 1), the legal basis for the personal-data-driven economy exists in a series of "legal bubbles", which "may eventually turn out to be unstable" due to the expansion of this industry on the *assumption* that courts would support the appropriation of personal data by these businesses after the fact, "turning their technological control of personal data into legally protected property rights". Notably, it has been suggested that the more recent turn to ethics in artificial intelligence (AI) policy is due to the absence of any internationally agreed AI framework (Chang, 2021). This instability makes the investigation of policy proposals and the way they represent policy problems especially important, as they can both point to, or influence, current trajectories in the development of regulation, its interpretation and implementation. More broadly, the paper points to an "illiberal drift" (Tréguer 2017) in which democratic states now enact forms of surveillance once unfathomable to previous generations. How certain technologies and surveillance practices are framed, toned down or 'disappeared' from policy discussions has important implications for our ability to resist or refuse them. The paper will: first, review the relevant literature; second; outline the theoretical and methodological approach; third, outline the case of the OECD; fourth, present the analysis; and fifth, provide a concluding discussion.

Literature overview

In the EU, the surveillance of populations is constrained by Article 8 of the *European Convention on Human Rights* (Council of Europe, 1950), the right to the protection of personal data under Article 8 of the *Charter of Fundamental Rights of the European Union* (2012) and the intention of the EU's GDPR to protect people's "fundamental rights and freedoms" (Article 1(2)). However, governments regularly track, collect, retain and correlate people's behaviour in their general management of

populations. Examples of these, both in Europe and around the world, include the administration of welfare (Higgs, 2003; Schram et al., 2009), healthcare (Sorell & Draper, 2012; French, 2014), policing (Ericson & Haggerty, 1997; Marda & Narayan, 2020), pandemic responses (French & Monahan, 2020), education (Taylor & Rooney, 2016) and aged care (Kenner, 2002). Since 2019, the use of automated decision-making and facial recognition systems by governments has increased, in most cases with a lack of transparency (AlgorithmWatch, 2019; AlgorithmWatch, 2020).

In the private sector, surveillance technologies are used, for example, in children's toys (Holloway, 2019), domestic appliances (Sadowski et al., 2021), domestic drones (Bracken-Roche, 2016), online price discrimination (Zuiderveen Borgesius & Poort, 2017), real time bidding for online advertising space (Irish Council for Civil Liberties, 2020; Veale & Zuiderveen Borgesius, 2022), and for the extraction of data from sensors installed in "smart homes" to inform pricing policies in sectors such as finance, insurance and real estate and to incentivise "good" behaviours by punishing the "bad" (Maalsen & Sadowski, 2019). Private companies are increasingly reliant on surveillance practices built into their business models which reflects a new political-economic order with surveillance at its core (Becker & Stalder, 2009; Zuboff, 2015; Srnicek, 2016; O'Neil, 2016; Lyon, 2022). Public-private partnerships, such as in 'smart cities', require enormous amounts of data to achieve public management goals and blur public/private lines of data ownership and accountability, irrespective of worthy aims such as the minimisation of vehicular traffic or fire risk reduction (Murakami Wood, 2015; Murakami Wood & Mackinnon, 2019). Data brokers have established a lucrative trade in the predictive promise of "behavioural insights" inferred through profiling (Reviglio, 2022).

Some surveillance practices provide a protective dimension such as monitoring dementia patients or children. However, the relationship between care and control is complex: Lyon (2007, p. 3) has described this relationship as a "continuum", whereas Nelson and Garey (2009, p. 8) see it more as co-existent and therefore dialectical rather than dichotomous. Even when surveillance technologies are used in the pursuit of "well-being" or the "public interest" (OECD, 2019a), they can create unintended effects. These include categorisations inferred from unanticipated correlation (Hildebrandt, 2008; Leese, 2014), new intersectional categories of discrimination not covered by existing anti-discrimination legislation (Mann & Matzner, 2019), social sorting (Lyon, 2003) and the secret scoring of consumers, such as those with a high commercial value (Schmitz, 2014) or deemed economically vulnerable (Committee on Commerce, Science and Transport & Office of Oversight

and Investigations Majority Staff, 2013, pp. 5-6). Such practices have been shown to produce unfair outcomes for minority groups (Browne, 2015; Koopman, 2019) and asymmetric power relations due to "non-reciprocal visibility" (Haggerty & Samatas, 2010, p. 9). Bias and inequality in machine learning is a further concern (Wachter et al., 2021).

Dataveillance is identified as producing "chilling effects" with respect to participation in deliberative democracies, where even the fear of surveillance can produce "self-censorship, conformity or anticipatory obedience" (Büchi et al., 2022, p. 2). In addition to practices which undermine fundamental rights and freedoms, the tools of digital surveillance can undermine the political process itself, such as by influencing public policy opinion data (Howard et al., 2002). The use of voter profiles in voter management software has seen a shift from broad political messaging to the micro-targeting of voters (Bennett, 2015). Recommendation algorithms on streaming services and social media platforms are believed to create "filter bubbles" as well as recommend extremist rather than more moderate content (Whittaker et al., 2021). Combined with misinformation, these processes can thwart the deliberative function of parliaments. Concerns about the effect of digitalisation being "dangerous to genuine power sharing" is not new, along with the concern that built-in biases of large systems will "affect public policy in the direction of centralisation, concentration, monopoly, regimentation, and monocracy" (Lasswell, 1971, p. 195). Yet concerns that would once have stopped surveillance practices such as facial recognition dead in their tracks no longer have the necessary sway. What has changed? This study attempts to take a slice of digitalisation policy discourse from the 1950s to the present to shed light on how representations of certain surveillance practices have shifted from something unthinkable to inevitable. This shift in the balance lines of acceptable risk reflects a broader "illiberal drift" of democratic states (Tregúer, 2017).

Theoretical and methodological approach

The idea behind the What's the problem represented to be? (WPR) approach is that by studying policy solutions as problematisations or "problem representations", we can unearth their implicit assumptions (Bacchi 2012, Bacchi & Goodwin, 2016). These, in turn, have "implications that follow for how lives are imagined and lived", referred to as "lived effects" (Bacchi & Goodwin, 2016, p. 6). The problem representations identified in digitalisation policy, for example, can reveal implicit or explicit assumptions about surveillance. These assumptions vary, reflecting the contested nature of surveillance (Fuchs, 2010). They range from the idea of surveil-

lance as a totalitarian form of control, connected to the creation of informational power asymmetries (Andrejevic, 2014; Whitson, 2010) to surveillance practices which reflect a "caring or empowering dimension" (Boersma et al., 2014, p. 2; Monahan, 2010). They also vary with respect to their representation of technology as neutral or as a nonhuman agent (Latour, 2005), or with political qualities (Winner, 1980).

The WPR approach has been applied to related areas including to e-Government policies (Sundberg, 2019), automation in policy discourse (Germundsson, 2022), the digital citizen in educational imaginaries (Rahm, 2019), the use of data analytics to identify families for service intervention (Edwards et al., 2021), problem representations of risk in the GDPR (Padden & Öjehag-Pettersson, 2021) and to identify discriminatory effects in the GDPR's representation of biometric data (Bisztray et al., 2021). Through the identification of "problem representations", the WPR approach can help to identify both explicit and implicit assumptions which determine who and what is included, or excluded, by a particular policy proposal.

In summary, this study identifies the varying and at times conflicting representations of surveillance practices found in the digitalisation policy of the OECD and how these problem representations have changed over time. Specifically, the study engages Question 2 of the WPR approach, which uses Foucault's genealogical method to identify how particular problem representations came about. The historical methodology of genealogy aims to *de-inevitabilse* our present-day understandings of concepts, in this case those of surveillance practices, within data protection, digitalisation and artificial intelligence (AI) policy. That is, our present policy framework is not an inevitable point in a linear history, but one of many alternatives "formed in the confluence of encounters and chances, during the course of a precarious and fragile history" (Foucault, 1990, p. 37, as cited in Bacchi & Goodwin, 2016, p. 46). A genealogy seeks to unearth a "history of the present" (Foucault, 1977, p. 31) and the beliefs and assumptions which underlie concepts and practices we might otherwise take for granted or "tend to feel without history" (Foucault, 1984, p. 76). That is, how we have come to understand a particular practice or logic (Walters, 2012).

Although historical, a genealogy "does not pretend to go back in time and restore an unbroken continuity that operates beyond the dispersement of forgotten things" (Foucault, 1984, p. 81). Rather, genealogy "permits the discovery, under the unique aspect of a trait or a concept, of the myriad events through which — thanks to which — they were formed" (Foucault, 1984, p. 81). In other words, their emergence or "moment of arising", as opposed to their "origins" or "causality" (Foucault,

1977, pp. 148-150). A genealogy "highlights the battles that take place over knowledge" (Bacchi & Goodwin 2016, p. 46). It aims to break down the "singularity" of a thing into its "multiplicity of discourses" and the many heterogeneous elements which have combined for its emergence (Koopman, 2013, p. 4). Discourses bring subjects, objects and places into existence, making what might once have been unthinkable into new, governable 'truths' (Bacchi & Goodwin, 2016).

By employing this technique, this article seeks to identify moments of "emergence", "battles" or "twists and turns" (Bacchi & Goodwin, 2016, p. 46) which have given us digitalisation policy in its present form. For example, surveillance practices such as the constant tracking of privately owned cars, once *unthinkable* as an unacceptable transgression of the basic right of freedom of movement, are now acceptable through the rationality of efficiency. Genealogy is also useful in helping us understand how meanings (especially contested meanings) have emerged, receded or continue to battle it out. This understanding is necessary in order to question the apparent immutability of certain meanings and to open up possibilities for change. This process is thus "indispensable to transformation", either to provoke us to change or to refuse what we are (Koopman, 2013, p. 16). The study brings to the literature an understanding of the conflicting representations of surveillance within the digitalisation policy discourse of a single institution.

Digitalisation discourse: the case of the OECD

In this study, the method of genealogy is used to perceive how we have come to understand the particular practices or logics of *surveillance* within the computerisation and digitalisation discourse of the OECD. To do this, "problem representations" which have a bearing on surveillance practices or which house explicit or implicit assumptions about surveillance practices have been identified in OECD policy documents over the past fifty years. Although documents from the late 1950s are included in the study, it is not until the early 1970s that surveillance appears as a policy problem in OECD material in relation to transborder data flows.

The OECD was chosen for three main reasons. Firstly, the OECD produced the first internationally agreed data protection principles, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, which were updated in 2013. Secondly, the transatlantic policy discussions facilitated by the OECD (published as a series of twelve *Informatics Studies*) in the lead up to the publication of the Privacy Guidelines offer a window into the underlying tensions between the dual aims of protecting both human rights and data flows. Thirdly, the OECD continues to play a role in the development of data protection, information technolo-

gy and artificial intelligence (AI) policy and has a co-operative relationship with the European Commission. The OECD is one of several organisations with a relatively long history with respect to digitalisation and is an interesting case because it offers insights into the development of the economic model of "surveillance capitalism" (Zuboff, 2019), for example, by floating the idea of using targeted (surveillance) advertising as one of several possible funding models to pay for internet content (OECD, 2006, p. 4).

The limitations of the study should be highlighted here. In theory, such a study could extend to all data protection policy discussion and debate from any organisation or jurisdiction. This study, however, is but one slice of a now very large digitalisation corpora. In Flyvberg's terms, it could be considered an "exemplar" or "paradigmatic case", which highlights more general characteristics of the subject of study and functions as a reference point for future enquiry (Flyvbjerg, 2006, p. 232). The documents included in the study cover the topics of computerisation, data protection, digitalisation, smart cities and artificial intelligence (AI). A broad sweep of OECD documents were first searched using the QSR Software application NVivo (released in 2018) to identify problem representations of the harms or benefits of surveillance practices. This initial search included all 463 of the OECD's legal instruments from 1957-2022 (both abrogated and in force), the twelve *Informatics Studies* from 1971-1978 (being policy papers and conference proceedings preceding the publication of the 1980 Guidelines), the 350 policy documents published under the rubric *OECD Digital Economy Papers* from 1985-2022 and eight publications from 2018-2021 concerning 'smart cities'. From this initial search, a set of documents were identified for closer analysis. These are listed in a table (Appendix 1). Coding focused on problem representations where policy whose solutions directly named or housed assumptions about surveillance practices, such as their potentially positive or negative effects. For the purpose of the study, the OECD publications are considered 'primary documents'. Publications upon which the OECD materials draw are referred to as 'secondary documents'. These can include references to legislation, scholarship and government inquiries which informed the OECD's work and which are useful in situating the primary documents in their historical context.

It should also be noted that it is not the aim of this article to provide a history of data protection policy or law. Rather, the study identifies and compares representations of surveillance in the policy solutions of selected OECD material in order to trace changes and show the sometimes contradictory ways in which surveillance is understood or problematised. The aim of the study, therefore, is to identify any

shifts in how surveillance is represented in the documents by selecting examples of texts which highlight changes. In doing so, the study highlights the *contingency* of our understanding of surveillance practices as something compatible, incompatible or tolerable in democratic states.

Analysis: problem representations of surveillance in OECD policy discourse

Problem representations of surveillance within the OECD documents are presented in the following section. Two overarching problem representations within digitalisation policy from the 1970s to the present day are the need to remove barriers to the free movement of data on the one hand, and the need to protect fundamental rights and freedoms whilst processing this data on the other (OECD, 1971, p. 21). It is within this second overarching problem representation, the protection of democratic rights and freedoms, where problem representations of surveillance are generally found. In the analysis to follow, negative representations of surveillance are shown in relation to oppressive effects of being overly efficient, the thwarting of individual or personal growth and the fear of creating a dystopian surveillance society. Neutral or positive representations of surveillance are then identified when surveillance practices are rebranded as neutral tools to promote efficiency, the public interest or even democracy itself. Practices held up as dystopian in one decade yet accepted as common practice in another provide explicit examples of this shift. Finally, representation of certain surveillance practices as inevitable is discussed, as well as the implications for resistance.

The problem of being too efficient

Although the tension between the two overarching objectives of free movement and the protection of fundamental rights and freedoms was already clear in the 1970s, problem representations of surveillance, especially of mass surveillance, were generally consistent, concurring that mass surveillance was an extreme to be avoided. For example, although standardised numbering systems such as national personal identification numbers were considered likely to provide economies of scale, they were cautioned *against* on the basis that they were "a major step towards potential surveillance of natural persons on a large scale" (OECD & Thomas, 1971, p. 22). Hesitancy was thus expressed in the means chosen to achieve efficiency if this meant the ability to connect previously dispersed information via a central record such as a personal number. The connection of information in this way was considered repugnant "because it facilitates considerably the building up of *personal dossiers* inside and outside public administration". It may sound odd

coming from an organisation whose mission is economic development, but in this case a *less* efficient system, with multiple records housed in unconnected filing systems, was preferred. This view reflected the broad consensus that the ability to create "personal dossiers" (i.e. profiles) was a bad thing in and of itself (OECD & Thomas, 1971, p. 22). However, this consensus shifts over the decades, with the advent of new technologies bearing offerings of efficiency and prediction too good to refuse.

Limiting an individual's potential to grow or change

It is in the documents of the 1970s where we find the most overt concern with surveillance. One important consideration was the idea that individual human development would somehow be stifled by data retention, making it impossible to close the "gap" between one's desires and what one is. Alan Westin's *Privacy and Freedom*, first published in 1967, is cited to make this point: "Faced with a continuous feedback of his previous acts, omissions and imperfections frozen in the indelible memory of a computer, the individual will find this gap more difficult to close than ever before" (OECD, 1971, p. 38). A decentralised "state of muddle or confusion in which the individual's private affairs are largely obscured" was regarded as preferable to a central collection and ordering of an individual's affairs, which was considered a "danger". It was deemed a problem to create "a condition in which the individual is subject to a feedback of almost unlimited information about himself and his actions" which would then produce a "danger that in the state of increased negentropy (…) the individual will lose degrees of freedom that he enjoys at present. In particular the freedom to grow" (OECD & Thomas, 1971, p. 38).

The views of Westin in relation to individual potential which are drawn on in the OECD material, reflect concerns of preceding decades with respect to the effect of automation. In 1958, political scientist Harold Lasswell (1958, p. 9) delivered a paper to the annual Western Joint Computer Conference on "the social consequences of automation", warning that "the installation of automatically monitored surveillance instruments" would limit privacy and "redouble the pressures toward cautious conformity" with respect to both legal rules and social convention. Without "limits" or "codes of freedom":

> The world will be comfortable only for people who have no unconventional impulses, no unpretty habits, no objectionable behaviours of any kind, no novel conceptions of rectitude. Man will be approaching the time when he automises himself into conformity, into seeming rectitude. Paradoxically, a license to be

> unobserved for awhile may become one of the principal rewards of meritorious conformity (Lasswell, 1958, p. 9).

Concerns of the 1950s were directed mostly toward the threat posed by automation to existing jobs and industries. However, by the 1970s, awareness of the scope of societal change due to computing was becoming more apparent, including the possibility of threatening the gains made in the preceding decades with respect to "personal freedom" of "speech, religion [and] assembly" (Ralston, 1973, p. 19). Lasswell's observations, like Westin's, move beyond the anticipated loss of personal freedoms, touching on aspects of governing in relation to these freedoms, whereby governmental rationalities excise non-conformist behaviour for its inefficiencies, whilst shaping "pretty" habits.

The surveillance possibilities of real-time computing systems also rang alarm bells in this respect:

> The real time information system is a new class of social institution, a more radically powerful and rapidly responsive social form to recognise, meet and deal with specified problems at the time they occur and in time to modify their outcome. If we neglect to formulate desirable social consequences for these new systems, we neglect them at our own peril, and at public peril (Sackman, 1971, p. 223).

Thus this "new class of social institution" was seen as having the potential to produce unfair power relations and negative effects on civil liberties, especially in the case of real time information systems due to their ability to steer or govern us by identifying "specified problems" for the purpose of correction or modification of behaviour as they occur, enabling real time "social control" or experimentation with the potential for "rigged choices" (Sackman, 1971, p. 235).

Orwellian visions of a transparent world

Data protection discussions from fifty years ago sound strikingly familiar to those of the present-day: a description of an "information explosion" followed by a list of all the ways computerisation and digitisation of information present new possibilities for increased storage, indexing and correlation as well as the challenges these processes raise for information security and privacy (OECD, 1971, pp. 9-12). More evident in this earlier literature, however, is a palpable fear associated with tech-

niques such as the digital storage of information given its potential to be used for surveillance purposes (Lasswell, 1958; Sackman, 1971). George Orwell's *Nineteen-Eighty Four,* published in 1949, loomed large in the public imagination in the 1960s and 1970s. The name Orwell is mentioned regularly in both the OECD material and in the secondary documents as a trope of totalitarian dystopia to warn of "a society vulnerable to a concentration of economic and political power (Orwell's 1984 scenario)" (OECD, 1976, p. 82). By calling on Orwell, politicians could expect to garner immediate and bipartisan agreement, as did Lord Baker, a conservative MP, when speaking on the UK Data Surveillance Bill 1969 and which is reproduced in full in the OECD publication in *Digital Information and the Privacy Problem* (OECD, 1971): "I do not want to sound alarmist, but George Orwell's nightmare of 1984 could easily come about by misuse of computers" (Column 286, 1969). The human rights abuses of World War II were also alive in the recent historical memory of the authors of the OECD's 1980 *Guidelines* on transborder data flows and the protection of privacy. According to the Chair of the OECD expert group which formulated the *Guidelines* (1978–80), stories circulating at the time about forgeries of blank ID cards to aid the Dutch resistance highlighted the dangers of identity systems being *too good to evade* in times of persecution (M. Kirby, personal communication, May 16, 2020).

Reference is made in the *Informatics Studies* to anti-surveillance currents on both sides of the Atlantic. Secondary documents cited include the 1966-1968 US Senate and Congressional Sub-committee hearings on the establishment of a US Government data centre. One excerpt from these hearings is described as exemplifying "the privacy problem" of the time (OECD & Thomas 1971, p. 17). Specifically, the nightmare scenario of a surveillance society as the ultimate taboo:

> The computer, with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may be come the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer (Prof. Arthur Miller, Statement to the US Senate, 1967, as cited in OECD, 1971, p. 17).

The view that computers had some new property or "dangerous *quality"* to them suggested that these machines, their new forms of information and their effects were not necessarily neutral:

> It is the ability of the computer to reorganise information it stores, to evaluate it in novel ways, to use sophisticated techniques of association and correlation that constitutes a large part of the fear that is provoked. There is a sense in which the evaluation of a vast *quantity* of information imparts a new and potentially more dangerous *quality* to it (OECD, 1971, p. 18).

The computer is also described as transforming manually stored records from a "solid state" to a "gaseous state", producing a new type of information with "a mobility, a pervasiveness, an ability to be transformed more than before" (OECD, 1971, pp. 14-15).

However, despite the oft raised spectre of an Orwellian future in both the primary and secondary documents, along with the concern that surveillance and automation could stifle the ability of a person to escape their past, the *Informatics Studies* embraced the benefits of computer technology to solve pressing problems of humankind and to achieve "social progress" and improvements in "the quality of life in its broadest sense" (OECD, 1976, p. 9). Computing technology was seen as a solution to economic crises, such the oil crisis, able to promote "new growth opportunities" (OECD, 1976, p. 14). There was, on the one hand, a general fascination with big picture societal advancements in relation to health care, public administration and finance (including a "cashless society") and prediction of future services such as shopping from home and distance education (OECD, 1976, p. 53).On the other hand, concern was expressed over the "social disadvantages" of those systems, such as a banking system which might "create a complete electronic record of the financial transactions of all members of society and permit invasions of privacy, surveillance and violation of civil rights on an unprecedented scale" (OECD, 1976, p. 109).

The overarching policy problem of the time was how to develop the roadmap to get to this future (and deal with issues such as privacy along the way). A sense of urgency also underpinned the need to move forward with harmonised regulation, given that "[w]e are in the midst of a sometimes painful transition from an industrial society to a post-industrial society" (OECD, 1976, p. 22) organised not around energy but "around information and the utilisation of information on the basis of organising the flow of knowledge" (Bell, 1976, as cited in OECD, 1976, p. 14). There is a strong sense in the documents that the shift to an information age was an inevitable stage of human progress. In facing this new stage, OECD member countries were keen to gain a competitive advantage in emerging computing markets at a time when "even developed countries could become economic backwaters"

(OECD, 1976, p. 14). No longer in the "golden age" of the post-war years, 1973-1989 is considered one of "cautious objectives", during which OECD GDP growth fell from 5% to 2.6%, which meant that non-OECD countries were growing at a faster rate (Clifton & Díaz-Fuentes, 2011). At the same time, exports fell from 9% to 2.6% and unemployment rose from 2.6% to 5.6% (Clifton & Díaz-Fuentes, 2011). In the concluding statements of a 1975 conference on computing and telecommunications policy, it was considered that: "Although there are many problems to be solved in dealing with an evolving information society, there was general agreement that mankind will be able to master the process of change and thus control his destiny" (OECD, 1976, p. 86). However, it is clear that for the policymakers of the 1970s, this mastery did *not* include harnessing surveillance practices to solve social and economic problems. Notably, this view is strongest across the board *before* the possibilities offered by NoSQL (non-relational) databases when combined with big data and real-time web applications began to appear in the 1990s.

The 1980 Privacy Guidelines

After a decade of intense work on computerisation, data protection and privacy, 1980 marked the publication of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The Council of Europe (1981) would adopt the first international treaty on data protection and privacy, Convention 108, the following year. The development of the OECD Guidelines had arisen due to concerns about inconsistent or competing data protection laws of member states which had become problematic due to the rise in automated processing, the need to ensure the free flow of data across national borders and "a common interest in protecting privacy and individual liberties" (OECD, 2011, p. 7). A Declaration on Transborder Data Flows in 1985 reinforced the commitment of member states to the OECD Guidelines and to promoting access to data and information-related services seen as key to economic growth (OECD, 1985). So the main work of the 1980s can be seen as promoting computerisation and harmonisation of legal frameworks to foster growth in this area, with expected economic benefits. The 1980s represented a moment to rest on their data protection laurels, given "the significant progress that has been achieved in the area of privacy protection at national and international levels" (OECD, 1985). The Guidelines, like today's work on 'data ethics' and 'trustworthy AI', aimed to quell privacy concerns associated with computing by implementing data protection principles to minimise risk to individual rights.

Profitability and rebranding of surveillance practices

During the 1980s, developments in computing technologies led to a rise in computer use, both in business and in the home. The internet was born, along with personal computers, office workstations, floppy disk drives, CD-ROMs, electronic games and desktop publishing (Computer History Museum, 2023). The 1990s continued this long line of new things with the "world wide web", photo and video editing software and palm pilots (Computer History Museum, 2023). By the end of 1996, web users had reached 36 million and this figure would reach 360 million by the end of the decade (Computer History Museum, 2023). An economic recession in the early 1990s helped re-emphasise the economic importance of new computing possibilities despite earlier concerns over the implications of computing for privacy and human rights. Surveillance practices once dismissed as anti-democratic began to be rebranded, lending them greater acceptability.

In tracing this rebranding from the 1970s to the present, it is particularly interesting to see how the potentially "dangerous" practices of one generation can become the essential services of the next. One cautionary example is the "dangerous" future scenario where hotel guest records have been correlated to show "the successive movements of a particular individual or group of individuals from one hotel to another" (OECD, 1971, p. 18). It is notable that in 1971 the retention and correlation of information about peoples' geographical movements is considered an *obvious problem,* yet since the mid 1990s hotel, flight and other travel services have been promoted as a benefit for the consumer, enabling responsiveness and customisation.

A second example from an abhorrent possible future is that of computer-based record-keeping in education:

> ...the replies of the pupil can be collected and permanently stored. These replies can be evaluated by the computer, perhaps correlated with the books the student has taken from the library (also stored by the computer) or with medical or psychological records. Finally the resulting information may be transmitted to unauthorised persons for example to the student's employer. There is a danger that the student will be judged, perhaps irrevocably and without his knowing it, by his responses to the computer, and his opportunities of employment may thereby be permanently affected (OECD, 1971, p. 19).

In 1971, the *idea* of systems to track and record the progress of students was seen as a *policy problem,* given such a system's potential to produce unjust outcomes for

students. By 1993, computerised systems were being used for school report and record writing (Wilson & Armstrong, 1993). In 2022 the global education software market was valued at over 123 billion USD and is expected to more than double in size by 2030 (Grand View Research, 2023).

"Surveillance capitalism" as a policy choice

The promise of once maligned surveillance practices saw them gain greater acceptability as a problem to be managed in order to reap economic benefits or even utilise them to 'pay' for digital goods and services. As an organisation to support economic growth, attention turned to supporting the internet as fundamental to the growth of the global economy (OECD, 2008b, p. 23). Whereas the OECD papers of the 1970s rejected surveillance practices because of their propensity to stifle individual growth and democratic freedoms such as those of movement or association, by the early 2000s surveillance practices were being supported as a means of paying for 'free' services and to promote economic growth. Targeted advertising, for example, was not always destined to be coupled to internet use. In 2006, discussion was still ongoing as to which business model would prevail in relation to the delivery of content. "Pay-per-view, prescription [subscription], free content and targeted advertisement" were seen as the main contenders, although it was anticipated that a combination of these would eventuate (OECD, 2006, p. 4). Customer loyalty programmes, for example, had already been identified as a means to "create extensive databases…to profile people's hobbies" and identify potential target markets (OECD, 1999, p. 50). Important here is that surveillance features such as those utilised in targeted marketing were not inevitable, but a deliberate policy choice. This choice helped to produce the internet as a space of surveillance. The Seoul Declaration committed OECD member states to a vision of the "internet economy" as a way to improve "employment, productivity, education, health and public services" as well as to "address global challenges, such as climate change" (OECD, 2008a, p. 4) Commitment to an internet economy dependent on profiling would deepen the tracks of surveillance technologies embedded in people's everyday experience, tracking more and more detailed aspects of everyday lives.

Thus from the mid-1990s, a shift can be seen in the OECD documents in which the problem representations of surveillance move away from being outright unacceptable and towards a more conditional tolerance or acceptability. Surveillance practices with the potential to be profitable and rejuvenate economies are rebranded as tools for better efficiency (OECD, 1997; OECD, 2022), transparency (OECD, 2000; OECD, 2022) convenience and customisation (OECD, 2018, p. 4; OECD, 2019c, p. 128). Policy responses to the 2007-2008 financial crisis reinforced the promotion

of investment in the digital economy and "smart infrastructure" (Guellec & Wunsch-Vincent, 2009, p. 5).

Surveillance in the 'public interest'

A particularly distinct contrast to the anti-surveillance stance of the 1970s can be found in the literature exploring strategies to combat the Covid-19 pandemic. Imagined in a context other than the 'public interest' (managing Covid outbreaks) the following excerpt paints a disturbing picture of the combined surveillance capabilities of public/private partnerships in relation to real-time tracking and tracing:

> A number of countries are using population surveillance to monitor COVID-19 in cases (for example, in Korea algorithms use geolocation data, surveillance-camera footage and credit card records to trace coronavirus patients). China assigns a risk level (colour code – red, yellow or green) to each person indicating contagion risk using cell phone software. While machine learning models use travel, payment, and communications data to predict the location of the next outbreak, and inform border checks, search engines and social media are also helping to track the disease in real-time (OECD, 2020b, p. 3).

Prior to the pandemic, desensitisation to mass surveillance practices by governments was a tendency already underway in relation to counterterrorism strategies, especially following 9/11 (Lyon 2001; Ball & Webster, 2003; Haggerty & Samatas, 2010, p. 10). Whereas the post-9/11 expansion of surveillance has occurred in a process of securitisation (Bigo, 2014), the current turn toward "ethical" and "trustworthy AI" emphasises the perceived benefits of surveillance practices to better organise society (OECD, 2021). Surveillance practices once considered intolerable for their potential to undermine the rights and possibilities for individuals in democratic societies are no longer rejected outright, but have become 'risks' to be managed, tolerable, neutral, or even desirable in their rebranding. For example, the SWOT analysis in the OECD Smart Cities Report for Inclusive Growth lists "possible abuse of citizen data, privacy and safety" as one of several "threats" posed by smart city initiatives which can be managed to reap perceived benefits in the public interest (OECD, 2020a, p. 18).

Inevitability and Resistance

The transformation of surveillance from something unacceptable to necessary is often accompanied by a notion of inevitability in connection with our "digital fu-

ture" (OECD, 2018, 2019a, 2019c). This is important because the notion of inevitability functions as an impediment to resisting surveillance practices coupled to our 'digital future'. As the rise in ubiquitous monitoring in society was linked to greater productivity and economic growth, it joined other technological developments as inevitable progress. For example, Radio Frequency Identity (RFID) tags embedded with small wireless sensors have been in use since the 1970s. They were first used to monitor rail carriages, but by the early 2000s had become common in transport, access control, event ticketing, identity cards, passports, manufacturing supply chains and distribution logistics (OECD, 2008b, p. 16). In a report developed to support the objectives of the Seoul Declaration on the Future of the Internet Economy in 2006, RFID tags are described as "a first step in the direction of "ubiquitous networked societies" (OECD, 2008b, p. 16). It is then stated that their use will (as if naturally) expand to enable "distance monitoring of ambient conditions" (temperature, pressure) and be used in a myriad of new applications, such as in health care and the environment. The development of a "ubiquitous networked society" is thus presented in a technologically determinist fashion, as if an inevitable step in humankind's progress, rather than one of several policy choices. Surveillance aspects, such as the ability of RFID devices to "trace and profile individuals", are noted as well as the possibility that public concern will be inflamed if RFID "tags and readers become pervasive and are combined with sensors and networks" (OECD, 2008b, p. 16). Informing consumers of related risks is proposed as a solution (OECD, 2008b, p. 17), although these solutions focus on the level of individual choice and control of individual privacy incursions rather than broader implications for society and democratic freedoms. The presentation of digitalisation as inevitable and *ipso facto* impossible to reject serves to limit the space given in the documents to refuse surveillance practices.

At other times, the documents show a 'resistance to resistance'. That is, their problem representations push back against concerns raised by civil society and academia which critique the widespread rise of surveillance practices. Following the Snowden revelations of illegal mass surveillance of individuals' electronic communications and 'hidden complicity' between government agencies and private providers, publications turn to the importance of consumer trust. One report promoting industry self-regulation put its main focus on how self-regulation can best address consumer issues, such as by developing advertising codes using 'trustmarks' (OECD, 2015b). Another appears to push back against privacy concerns, proposing "balanced" approaches to "protecting competition, consumers and privacy" when striving for internet openness (technical, economic and social openness) seen as necessary for economic growth, social well-being, international trade, in-

novation and macroeconomic performance (OECD, 2016, pp. 5-14). Without directly naming the case, the documents respond to high profile breaches of trust such as Cambridge Analytica's illegal use of 87 million Facebook profiles to micro-target voters (OECD, 2019b, p. 20).

The Seoul Declaration recognises the need for OECD member countries to defend broader processes of digitalisation when trust is threatened:

> The confidence of the end user is essential to building that trust and to the continued growth of the Internet economy. When it is shaken, even mildly, it is difficult to regain. To prevent loss of confidence, policies and measures are needed, from increasing the security of information systems and networks to creating trustworthy digital identities, to protecting consumers, personal information, minors and other vulnerable groups, and more broadly to fostering transparency and fairness (OECD, 2008a).

The principal reason given for the policies and measures to promote transparency and fairness is to maintain confidence in the economy. This is not unlike the promotion of data protection and privacy policies in the 1970s to allay fears at the time that computerisation would create Orwellian-style intrusions into individual privacy.

In summary, over the past fifty years, problem representations in the OECD material show a greater acceptance, if not tolerance, of surveillance practices once deemed unacceptable. This shift is by no means clear-cut, but a tension or wrestling back-and-forth over time, and which still continues. An overarching shift, however, is best reflected in the changing representations of surveillance practices in the 1970s from an extreme to be avoided in order to prevent "a society vulnerable to a concentration of economic and political power (Orwell's 1984 scenario)" (OECD, 1976, p. 82) to a society embracing "trustworthy AI" (OECD, 2021). Ultimately, we see a kind of *doublethink* throughout the OECD policy discourse on digitalisation, where surveillance practices can at once be conceived as undemocratic (OECD, 1976, p. 9) *and* as systems to serve humankind; to "promote shared well-being and prosperity while protecting individual rights and democratic values" (OECD, 2021, p. 4). What changes over time is the position of surveillance practices on the slide rule of acceptability and the balancing lines of 'public interest' and economic 'well-being' versus individual rights,democratic freedoms, and social 'well-being'. The implications of this shift are taken up in the discussion which follows.

Concluding discussion

This article has sought to show changes in the problem representations of surveillance, specifically the surveillance practices of dataveillance, in the digitalisation discourse of the OECD over the past fifty years. The study highlights a transformation that is still underway. That is, how understandings of surveillance practices have shifted or are shifting from being a policy *problem* — posed as a clear and present danger to democratic rights and freedoms — to a policy *solution* as a "tool for improving lives" (OECD, 2019c). As noted above, the study does not make claims in relation to digitalisation discourse beyond the OECD, although given the composition of OECD membership certain similarities with other western organisations or states could be expected. Similar studies of other corpora, such as the Council of Europe, European Commission, or national policies, would enable a comparison of the representations of surveillance practices, including any differences in acceptability or tolerance.

Whilst certain surveillance practices continue to be raised as problematic in the OECD literature, concerns have become less stringent, shying away from rejecting surveillance outright as antithetical to democracy. A watering down of earlier views is pragmatic and helps minimise opposition to the use of surveillance practices to achieve economic growth. Although the self-censorship, or "chilling effects", of surveillance practices such as tracking, monitoring or data retention are well documented (Richards, 2013) and discussed as a possible harm in our AI future (OECD, 2019c, p. 110), they are represented as "risks to be managed" (OECD, 2015a; OECD, 2019c, p. 26) and no longer as reasons for refusal, as they were in earlier decades. Increasing emphasis is placed on the potential of surveillance practices to *improve* society, whilst "upholding democratic values" (OECD, 2021, p. 6). The rebranding of surveillance practices in digitalisation discourse from something bad to something manageable, neutral, or even positive, is reliant upon the assumption that surveillance practices are themselves neutral. That is, in addition to being potentially *dangerous* they can be *fair*, *ethical* or *trustworthy*. Surveillance practices, once considered incompatible with democracy, are now considered one of many "ethical and fairness concerns" among which "respect for human rights and democratic values" are also included (OECD, 2019a, p. 16). This is very different from being considered fundamentally anti-democratic and therefore untenable. Instead, a "balancing act" is called for between opportunity and risk (OECD, 2019c). Whilst a balancing act has always taken place in the area of data protection and privacy, the balance lines have shifted: Problem representations of the "dangers" of computerisation have changed over time, or have been 'invisibilised',

contributing not only to a greater tolerance of surveillance practices but to their promotion.

One important shift over time can be seen in the extent to which the OECD materials express concern over the discriminatory potential of feedback loops to limit a person's ability to grow or change. The notion that a person can grow and improve their lot in life through democratic freedoms which promote self-determination and self-development is associated with democratic theories stemming from Mill, Green and Dewey (Warren, 1992). Whilst this was an explicit concern in the earlier documents (OECD, 1971, p. 38) it disappears as a concern in relation to real-time information systems which are the lifeblood of smart cities and the Internet of Things. Koopman (2019) captures this earlier concern in his concept of *infopower*, describing how we are "pinned down" when our personal information is formatted: "Formats are acts of power that subject us to operations being fastened to data". This fastening happens twice: first in the process of being "canalised" by the format itself, such as a social media profile, and again when we are "accelerated" by the speed with which we find and navigate information (assisted by its common formats) (Koopman, 2019, pp. 156-157). Whereas a perpetually retrospective feedback loop to predict future behaviour was once *the* reason to dismiss outright what we now know as educational software, these types of concerns are now absent or reframed as "trust" and "fairness" issues which downplay the harms once associated with these types of systems in the OECD literature. Instead, the focus is now on minimising the risks to the fairness or increasing the transparency of algorithms processing past behaviour to generate insights or make decisions, rather than the questions of whether an algorithm should be used *at all*. According to Louise Amoore (2020), the algorithm is a site of future political protest: beyond concerns of data protection and privacy, algorithms use data to change people's futures without regard to individual personhood. Garfield (2020) asks what it will take "to send an AI system to the trash" and proposes a mapping of AI to identify criteria for refusal and resistance.

The transformation of surveillance from a self-evident evil to the engine room of the digital age has implications for our possibilities to resist the growing array of surveillance practices tied to digitalisation. In his genealogy of the "informational person", Koopman challenges us to imagine a situation where all our own personal data has been permanently erased (2019, p. ix). In such a predicament, the inability of a person to function in society highlights the dependency we now have upon our data and the near impossibility of refusing it. When dataveillance is tied to digitalisation, the possibility to refuse dataveillance practices is also reduced. Ac-

cording to Koopman (2019, p. ix), the past holds moments "when data was not yet closed, but rather glaringly open to contestation and recomposition". In the early 1970s, a "Great Refusal of Technetronic Society" still seemed open, even if likely to be repressed as a foolish counter-revolutionary effort, a "last spasm of the past", in the vein of "peasants, Luddites and Chartists" resisting the industrial age (Mendel, 1971, p. 168). Although computerisation was presented as an *inevitable* step in humankind's progress and desirable as an engine for economic growth and rationalisation in the OECD policy discourse of the 1970s, resisting certain surveillance practices within this future still seemed feasible, especially when ubiquitous computing was still a sci-fi future and not a material policy choice.

Refusal of our present moment, amidst a great "digital transformation" (OECD, 2019c), seems more difficult, although not impossible. Surveillance practices such as behavioural advertising *are* being challenged. For example, the July 2023 decision by the Court of Justice of the European Union that Meta has conducted illegal behavioural advertising and demonstrated "an abuse of a dominant position" (Court of Justice of the European Union, 2023). Notably, the court questioned the consent obtained by Meta to process users' data "since that [dominant] position is liable to affect the freedom of choice of those users and create a clear imbalance between them and the data controller" (Court of Justice of the European Union, 2023). In light of this decision, the Norwegian Data Protection Authority has placed a temporary ban placed on "behavioural advertising based on the surveillance and profiling of users in Norway" by Meta on Facebook and Instagram, condemning behavioural advertising for curtailing "freedom of expression and freedom of information in society" (Datatilsynet, 2023).

In summary, the aim of this paper has been to draw attention to the way in which the representation of surveillance practices has transformed over the past fifty years in one particular corpora, the OECD. By bringing attention to the rebranding of surveillance practices once maligned as the thin edge of a totalitarian wedge, it is hoped to highlight the surveillance aspects of digitalisation as contingent, rather than inevitable, and which can therefore be resisted or refused. Identifying changes in our representation and understanding of surveillance practices helps to show how it has been possible to shift from thinking of surveillance practices as an obvious problem, to their normalisation (Levy, 2015). If surveillance practices can potentially undermine democratic systems of government, then it is necessary to recognise this shift so as not to obscure the lived effects of practices which may remain, despite their rebranding, as well as to open up possibilities to question, resist or even refuse them.

ACKNOWLEDGMENTS

The author would like to thank the IPR reviewers of this article, Felix Tréguer and Urbano Reviglio, for their comprehensive and very helpful feedback. She would also like to thank Colin Koopman and Ethan Hallerman for their thoughtful comments on an earlier draft of this article presented at the fourth Critical Genealogies Workshop.

References

AlgorithmWatch. (2019). *Automating society – Taking stock of automated decision-making in the EU* [Report]. AlgorithmWatch; Bertelsmann Stiftung. https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf

AlgorithmWatch. (2020). *Automating society report 2020* [Report]. AlgorithmWatch and Bertelsmann Stiftung. https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf

Amoore, L. (2020, August 19). Why 'Ditch the algorithm' is the future of political protest. *The Guardian*. https://www.theguardian.com/commentisfree/2020/aug/19/ditch-the-algorithm-generation-students-a-levels-politics

Andrejevic, M. (2014). Big data, big questions: The big data divide. *International Journal of Communication*, *8*, 1673–1689.

Bacchi, C. (2009). *Analysing policy: What's the problem represented to be?* Pearson Education.

Bacchi, C. (2012). Why study problematizations? Making politics visible. *Open Journal of Political Science*, *2*(1), 1–8. https://doi.org/10.4236/ojps.2012.21001

Bacchi, C. L., & Goodwin, S. (2016). *Poststructural policy analysis: A guide to practice*. Palgrave Macmillan.

Baker, K. (1969, May 06). *Data surveillance* [Hansard] (Vol. 783). https://api.parliament.uk/historic-hansard/commons/1969/may/06/data-surveillance

Ball, K., & Webster, F. (Eds.). (2003). *The intensification of surveillance: Crime, terrorism and warfare in the information age*. Pluto Press. https://doi.org/10.2307/j.ctt18fs7k5

Becker, K., & Stalder, F. (Eds.). (2009). *Deep search: The politics of search beyond Google*. Studien Verlag.

Benjamin, G. (2020, December 11). *"Put it in the bin": Mapping AI as a framework of refusal*. Resistance AI Workshop at NeurIPS2020. https://pure.solent.ac.uk/en/publications/put-it-in-the-bin-mapping-ai-as-a-framework-of-refusal

Bennett, C. J. (2015). Trends in voter surveillance in Western societies: Privacy intrusions and democratic implications. *Surveillance & Society*, *13*(3/4), 370–384. https://doi.org/10.24908/ss.v13i3/4.5373

Bigo, D. (2014). The (in)securitization practices of the three universes of EU border control: Military/navy – border guards/police – database analysts. *Security Dialogue*, *45*(3), 209–225. https://doi.org/10.1177/0967010614530459

Bisztray, T., Gruschka, N., Bourlai, T., & Fritsch, L. (2021). Emerging biometric modalities and their use: Loopholes in the terminology of the GDPR and resulting privacy risks. *International Conference of the Biometrics Special Interest Group (BIOSIG)*, 1–5. https://doi.org/10.1109/BIOSIG52210.2021.9548298

Boersma, K., Brakel, R., Fonio, C., & Wagenaar, P. (2014). *Histories of state surveillance in Europe and beyond*. Routledge. https://doi.org/10.4324/9780203366134

Bracken-Roche, C. (2016). Domestic drones: The politics of verticality and the surveillance industrial complex. *Geographica Helvetica*, *71*(3), 167–172. https://doi.org/10.5194/gh-71-167-2016

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press. https://read.dukeuprhttps://doi.org/10.1215/9780822375302ess.edu/books/book/147/

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society*, *9*(1), 205395172110653. https://doi.org/10.1177/20539517211065368

Chang, H. (2021). Responding to ethics being a data protection building block for AI. *Journal of AI, Robotics and Workplace Automation*, *1*(1). https://ssrn.com/abstract=3952753

Charter of fundamental rights of the European Union [C 326/02]. (2012). Official Journal of the European Union, 391–407. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512. https://doi.org/10.1145/42411.42413

Clifton, J., & Díaz-Fuentes, D. (2011). The OECD and phases in the international political economy, 1961–2011. *Review of International Political Economy*, *18*(5), 552–569. https://doi.org/10.1080/09692290.2011.620464

Committee on Commerce, Science and Transport & Office of Oversight and Investigations Majority Staff. (2013). *A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes* (pp. 1–36) [Staff report]. United States Senate. https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577

Computer History Museum. (2023). *Timeline of computer history*. https://www.computerhistory.org/timeline/

Council of Europe. (1950). *Convention for the protection of human rights and fundamental freedoms* (ETS no. 005). As amended by Protocol No- 15 (CETS no. 213). In force from 1 August 2021. https://www.echr.coe.int/documents/convention_eng.pdf

Council of Europe. (1981). *Convention for the protection of individuals with regard to automatic processing of personal data* (ETS No. 108). https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Court of Justice of the European Union. (2023). *Judgment of the court in case C-252/21. Meta platforms and others (general terms of use of a social network)* (Press Release No. 133/23). https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-07/cp230113en.pdf

Datatilsynet. (2023). *Temporary ban on behavioural advertising on Facebook and Instagram*. https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/temporary-ban-of-behavioural-advertising-on-facebook-and-instagram/

Edwards, R., Gillies, V., & Gorin, S. (2022). Problem-solving for problem-solving: Data analytics to identify families for service intervention. *Critical Social Policy*, *42*(2), 265–284. https://doi.org/10.1177/02610183211020294

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society*. University of Toronto Press. https://doi.org/10.3138/9781442678590

European Commission. (2021). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative Acts* (COM/2021/206 final). European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Parliament, Tecnalia Research and Investigation, Gamino Garcia, A., Cortes Velasco, C., Iturbe Zamalloa, E., Rios Velasco, E., Eguía Elejabarrieta, I., Herrera Lotero, J., & Larrañeta Ibañez, J. J. (2015). *Mass surveillance—Part 1: Risks, opportunities and mitigation strategies* [Study]. Scientific Foresight (STOA) Unit. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2015)527409

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry*, *12*(2), 219–245. https://doi.org/10.1177/1077800405284363

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Peregrine Books.

Foucault, M. (1984). Polemics, politics, and problematizations. In P. Rabinow (Ed.), *The Foucault Reader* (pp. 381–390). Pantheon Books.

French, M. (2014). Gaps in the gaze: Informatic practice and the work of public health surveillance. *Surveillance & Society*, *12*(2), 226–242. https://doi.org/10.24908/ss.v12i2.4750

French, M., & Monahan, T. (2020). Dis-ease surveillance: How might surveillance studies address COVID-19? *Surveillance & Society*, *18*(1), 1–11. https://doi.org/10.24908/ss.v18i1.13985

Fuchs, C. (2010). *How can surveillance be defined? Remarks on theoretical foundations of surveillance studies* (Research Paper 1; The Internet & Surveillance, pp. 1–22). http://sns3.uti.at/wp-content/uploads/2010/10/The-Internet-Surveillance-Research-Paper-Series-1-Christian-Fuchs-How-Surveillance-Can-Be-Defined.pdf

Germundsson, N. (2022). Promoting the digital future: The construction of digital automation in Swedish policy discourse on social assistance. *Critical Policy Studies*, *16*(4), 478–496. https://doi.org/10.1080/19460171.2021.2022507

Giraudo, M. (2020). On legal bubbles: Some thoughts on legal shockwaves at the core of the digital economy. *Journal of Institutional Economics*, *18*(4), 587–604. https://doi.org/10.2139/ssrn.3766713

Grand View Research. (2023). *Education technology market size, share & trends analysis report by sector (preschool, K-12, higher education), by end-user (business, consumer), by type, by deployment, by region, snd segment forecasts, 2023—2030* (p. 117) [Market analysis report]. https://www.grandviewresearch.com/industry-analysis/education-technology-market

Guellec, D., & Wunsch-Vincent, S. (2009). *Policy responses to the economic crisis: Investing in innovation for long-term growth* (Report 159; OECD Digital Economy Papers, Vol. 159). OECD

Publishing. https://doi.org/10.1787/222138024482

Haggerty, K. D., & Samatas, M. (2010). Introduction: Surveillance and democracy: An unsettled relationship. In K. D. Haggerty & M. Samatas (Eds.), *Surveillance and democracy*. Routledge-Cavendish. https://doi.org/10.4324/9780203852156

Higgs, E. (2003). *The informational state in England: The central collection of information on citizens since 1500*. Palgrave Macmillan.

Hildebrandt, M. (2008). Defining profiling: A new type of knowledge? In M. Hildebrandt & S. Gutwirth (Eds.), *Profiling the European citizen* (pp. 17–45). Springer. https://doi.org/10.1007/978-1-4020-6914-7_2

Holloway, D. (2019). Surveillance capitalism and children's data: The Internet of toys and things for children. *Media International Australia*, *170*(1), 27–36. https://doi.org/10.1177/1329878X19828205

Howard, P. N., Carr, J. N., & Milstein, T. J. (2002). Digital technology and the market for political surveillance. *Surveillance & Society*, *3*(1). https://doi.org/10.24908/ss.v3i1.3320

Irish Council Civil Liberties. (2020). *Two years of DPC inaction on the ongoing RTB data breach: Irish people with AIDS profiled, and Polish elections influenced* [Press statement]. https://www.iccl.ie/digital-data/rtb-data-breach-2-years-on/

Katzenbach, C., & Bächle, T. C. (2019). Defining concepts of the digital society. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1430

Kenner, A. M. (2002). Securing the elderly body: Dementia, surveillance, and the politics of 'aging in place'. *Surveillance & Society*, *5*(3). https://doi.org/10.24908/ss.v5i3.3423

Koopman, C. (2013). *Genealogy as critique: Foucault and the problems of modernity*. Indiana University Press. https://www.jstor.org/stable/j.ctt16gzmqf

Koopman, C. (2019). *How we became our data: A genealogy of the informational person*. University of Chicago Press.

Laswell, H. D. (1958). The social consequences of automation. *Proceedings of the May 6-8, 1958, Western Joint Computer Conference: Contrasts in Computers*, 7–10. https://doi.org/10.1145/1457769.1457772

Lasswell, H. D. (1971). Policy problems of a data-rich civilization. In A. F. Westin (Ed.), *Information technology in a democracy* (pp. 187–197). Harvard University Press. https://doi.org/10.4159/harvard.9780674436978.c29

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, *45*(5), 494–511. https://doi.org/10.1177/0967010614544204

Levy, K. E. C. (2015). Intimate surveillance. *Idaho Law Review*, *51*(3), 679–693.

Lyon, D. (2001). Surveillance after September 11. *Sociological Research Online*, *6*(3), 116–121. https://doi.org/10.5153/sro.643

Lyon, D. (Ed.). (2003). *Surveillance as social sorting: Privacy, risk and digital discrimination*. Routledge.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

Lyon, D. (2022). Surveillance. *Internet Policy Review*, *11*(4). https://doi.org/10.14763/2022.4.1673

Maalsen, S., & Sadowski, J. (2019). The smart home on FIRE: Amplifying and accelerating domestic surveillance. *Surveillance & Society*, *17*(1/2), 118–124. https://doi.org/10.24908/ss.v17i1/2.12925

Mann, M., & Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. *Big Data & Society*, *6*(2). https://doi.org/10.1177/2053951719895805

Marda, V., & Narayan, S. (2020). Data in New Delhi's predictive policing system. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 317–324. https://doi.org/10.1145/3351095.3372865

Mendel, A. P. (1971). The great refusal of technetronic society. In A. F. Westin (Ed.), *Information technology in a democracy*. Harvard University Press. https://doi.org/10.4159/harvard.9780674436978.c27

Monahan, T. (2010). Surveillance as governance: Social inequality and the pursuit of democratic surveillance. In K. D. Haggerty & M. Samatas (Eds.), *Surveillance and Democracy*. Routledge-Cavendish. https://doi.org/10.4324/9780203852156

Murakami Wood, D. (2015). *Smart city, surveillance city* [Opinion piece]. Society for Computers and Law. https://www.scl.org/articles/3405-smart-city-surveillance-city

Murakami Wood, D., & Mackinnon, D. (2019). Partial platforms and oligoptic surveillance in the smart city. *Surveillance & Society*, *17*(1/2), 176–182. https://doi.org/10.24908/ss.v17i1/2.13116

Nelson, M. K., & Garey, A. I. (Eds.). (2009). *Who's watching?: Daily practices of surveillance among contemporary families*. Vanderbilt University Press. https://doi.org/10.2307/j.ctv17vf76w

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.

Organisation for Economic Co-operation and Development. (n.d.). *About the OECD*. https://www.oecd.org/about/

Organisation for Economic Co-operation and Development. (1971). *Digital information and the privacy problem*.

Organisation for Economic Co-operation and Development. (1976). Conference on computer/telecommunications policy. *Proceedings of the OECD Conference, February 4-6, 1975*.

Organisation for Economic Co-operation and Development. (1980). Guidelines on the protection of privacy and transborder flows of personal data. In *OECD guidelines on the protection of privacy and transborder flows of personal data* (pp. 8–52). OECD Publishing. https://doi.org/10.1787/9789264196391-en

Organisation for Economic Co-operation and Development. (1985). *Declaration on transborder data flows* (Declaration 1; OECD Digital Economy Papers, Vol. 1). OECD Publishing. https://doi.org/10.1787/230240624407

Organisation for Economic Co-operation and Development. (1997). *Sacher report* (Report 29; OECD Digital Economy Papers, Vol. 29). OECD Publishing. https://doi.org/10.1787/237058611046

Organisation for Economic Co-operation and Development. (1999). *Economic and social impact of e-*

commerce: Preliminary findings and research agenda (Research Report 40; OECD Digital Economy Papers, Vol. 40). OECD Publishing. https://doi.org/10.1787/236588526334

Organisation for Economic Co-operation and Development. (2000). *Transborder data flow contracts in the wider framework of mechanisms for privacy protection on global networks* (Report 66; OECD Digital Economy Papers, Vol. 66). OECD Publishing. https://doi.org/10.1787/233311170363

Organisation for Economic Co-operation and Development. (2006). *Future digital economy: Digital content creation, distribution and access - Conference conclusions* (Report 118; OECD Digital Economy Papers, Vol. 118). OECD Publishing. https://doi.org/10.1787/231438658873

Organisation for Economic Co-operation and Development. (2008a). *Shaping policies for the future of the internet economy* (Report 148; OECD Digital Economy Papers, Vol. 148). OECD Publishing. http s://doi.org/10.1787/230388107607

Organisation for Economic Co-operation and Development. (2008b). *The Seoul declaration for the future of the internet economy* (Declaration 147; OECD Digital Economy Papers, Vol. 147). OECD Publishing. https://doi.org/10.1787/230445718605

Organisation for Economic Co-operation and Development. (2011). *The evolving privacy landscape: 30 years after the OECD privacy guidelines* (Report 176; OECD Digital Economy Papers, Vol. 176). OECD Publishing. https://doi.org/10.1787/5kgf09z90c31-en

Organisation for Economic Co-operation and Development. (2015a). *Data-driven innovation: Big data for growth and well-being*. OECD Publishing. https://doi.org/10.1787/9789264229358-en

Organisation for Economic Co-operation and Development. (2015b). *Industry self regulation: Role and use in supporting consumer interests* (Report 247; OECD Digital Economy Papers, Vol. 247). OECD Publishing. https://doi.org/10.1787/5js4k1fjqkwh-en

Organisation for Economic Co-operation and Development. (2016). *Economic and social benefits of internet openness* (Report 257; OECD Digital Economy Papers). OECD Publishing. https://doi.org/1 0.1787/5jlwqf2r97g5-en

Organisation for Economic Co-operation and Development. (2018). *Consumer policy and the smart home* (Report 268; OECD Digital Economy Papers). OECD Publishing. https://doi.org/10.1787/e124c 34a-en

Organisation for Economic Co-operation and Development. (2019a). *Artificial intelligence in society*. OECD Publishing. https://doi.org/10.1787/eedfee77-en

Organisation for Economic Co-operation and Development. (2019b). *Enhancing the Contribution of Digitalisation to the Smart Cities of the Future* [Report]. https://www.oecd.org/regional/regionaldevel opment/Smart-Cities-FINAL.pdf

Organisation for Economic Co-operation and Development. (2019c). *Going digital: Shaping policies, improving lives*. OECD Publishing. https://doi.org/10.1787/9789264312012-en

Organisation for Economic Co-operation and Development. (2020a). *Smart cities and inclusive growth: Building on the outcomes of the 1st OECD roundtable on smart cities and inclusive growth* [Report]. Organisation for Economic Co-operation and Development and the Ministry of Land, Infrastructure and Transport, Korea. https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Citi es_and_Inclusive_Growth.pdf

Organisation for Economic Co-operation and Development. (2020b). *Using artificial intelligence to help combat COVID-19* [Policy response]. Organisation for Economic Co-operation and Development.

https://read.oecd-ilibrary.org/view/?ref=130_130771-3jtyra9uoh&title=Using-artificial-intelligence-to-help-combat-COVID-19

Organisation for Economic Co-operation and Development. (2021). *Tools for trustworthy AI: A framework to compare implementation tools for trustworthy AI systems* (Report 312; OECD Digital Economy Papers). OECD Publishing. https://doi.org/10.1787/008232ec-en

Organisation for Economic Co-operation and Development. (2022). *OECD framework for the classification of AI systems* (Guidance 323; OECD Digital Economy Papers). OECD Publishing. https://doi.org/10.1787/cb6d9eca-en

Organisation for Economic Co-operation and Development, & Thomas, U. (1971). *Computerised data banks in public administration: Trends policies and issues*. Organisation for Economic Co-operation and Development.

Padden, M., & Öjehag-Pettersson, A. (2021). Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR). *Critical Policy Studies*, *15*(4), 486–503. https://doi.org/10.1080/19460171.2021.1927776

Privacy International. (2021). *Mass surveillance*. https://privacyinternational.org/learn/mass-surveillance

Rahm, L. (2019). *Educational imaginaries: A genealogy of the digital citizen* [Doctoral thesis, Linköping University]. https://doi.org/10.3384/diss.diva-154017

Ralston, A. G. (1973, April). Computers and democracy. *Computers and Automation and People*, *22*(4).

Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview. *Internet Policy Review*, *11*(3). https://doi.org/10.14763/2022.3.1670

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review*, *126*(7). https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/

Rule, J., McAdam, D., Stearns, L., & Uglow, D. (1980). *The politics of privacy*. New American Library.

Sackman, H. (1971). A public philosophy for real time information systems. In A. F. Westin (Ed.), *Information technology in a democracy* (pp. 222–236). Harvard University Press. https://doi.org/10.4159/harvard.9780674436978.c33

Sadowski, J., Strengers, Y., & Kennedy, J. (2021). More work for big mother: Revaluing care and control in smart homes. *Environment and Planning A: Economy and Space*, 0308518X2110223. https://doi.org/10.1177/0308518X211022366

Schmitz, A. J. (2014). *Secret consumer scores and segmentations: Separating 'haves' from 'have-nots'*. Social Science Research Network. https://ssrn.com/abstract=2617502

Schram, S. F., Soss, J., Fording, R. C., & Houser, L. (2009). Deciding to discipline: Race, choice, and punishment at the frontlines of welfare reform. *American Sociological Review*, *74*(3), 398–422. https://doi.org/10.1177/000312240907400304

Sorell, T., & Draper, H. (2012). Telecare, surveillance, and the welfare state. *The American Journal of Bioethics*, *12*(9), 36–44. https://doi.org/10.1080/15265161.2012.699137

Srnicek, N. (2017). *Platform capitalism*. Polity.

Sundberg, L. (2019). If digitalization is the solution, what is the problem? *Papers Presented at the*

19th European Conference on Digital Government ECDG 2019, 136–143. http://urn.kb.se/resolve?urn=urn:nbn:se:miun:diva-37597

Taylor, E., & Rooney, T. (2016). Digital playgrounds: Growing up in the surveillance age. In E. Taylor & T. Rooney (Eds.), *Surveillance futures: Social and ethical implications of new technologies for children and young people* (pp. 13–28). Routledge. https://doi.org/10.4324/9781315611402

Tréguer, F. (2017). Intelligence reform and the Snowden paradox: The case of France. *Media and Communication*, *5*(1), 17–28. https://doi.org/10.17645/mac.v5i1.821

Veale, M., & Borgesius, F. Z. (2022). Adtech and real-time bidding under European data protection law. *German Law Journal*, *23*(2), 226–256. https://doi.org/10.1017/glj.2022.18

Wachter, S., Mittelstadt, B., & Russell, C. (2021). Bias preservation in machine learning: The legality of fairness metrics under EU non-discrimination law. *West Virginia Law Review*, *123*(3), 734–790. https://doi.org/10.2139/ssrn.3792772

Walters, W. (2012). *Governmentality: Critical encounters*. Routledge.

Warren, M. (1992). Democratic theory and self-transformation. *American Political Science Review*, *86*(1), 8–23. https://doi.org/10.2307/1964012

Watt, E. (2017). The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, *21*(7), 773–799. https://doi.org/10.1080/13642987.2017.1298091

Whitson, J. R. (2010). Surveillance and democracy in the digital enclosure. In K. D. Haggerty & M. Samatas (Eds.), *Surveillance and Democracy*. Routledge-Cavendish. https://doi.org/10.4324/9780203852156

Whittaker, J., Looney, S., Reed, A., & Votta, F. (2021). Recommender systems and the amplification of extremist content. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1565

Wilson, B., & Armstrong, D. (1993). A computerized system for school report and record writing. *Computers & Education*, *21*(4), 321–330. https://doi.org/10.1016/0360-1315(93)90035-H

Winner, L. (1980). Do artefacts have politics? *Daedalus*, *109*(1), 121–166.

Zalnieriute, M. (2021). Big Brother Watch v. UK: Procedural fetishism and mass surveillance under the ECHR. *Verfassungsblog: On Matters Constitutional*. https://doi.org/10.17176/20210602-123858-0

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Zuiderveen Borgesius, F., & Poort, J. (2017). Online price discrimination and EU data privacy law. *Journal of Consumer Policy*, *40*(3), 347–366. https://doi.org/10.1007/s10603-017-9354-z

Appendix 1: The transformation of surveillance in the digitalisation discourse of the OECD: A brief genealogy

Table 1: Selected OECD documents

NO.	YEAR	DOCUMENT TITLE	DOCUMENT TYPE	BACKGROUND
1	1971	Computerised data banks in public administration: Trends policies and issues.	OECD Informatics Studies	OECD Informatics Studies No. 1. A report prepared by Uwe Thomas, Consultant to the OECD. The Informatics Studies were commissioned by the Computer Utilisation Group in response to the recommendations of the third OECD Ministerial Meeting on Science (1971) on a range of computing issues.
2	1971	Digital Information and the Privacy Problem	OECD Informatics Studies	Informatics Studies No. 2. Prepared by G.B.F. Niblett, Consultant to the OECD.
3	1973	Computers and Telecommunications: Economic, Technical and Organisational Issues	OECD Informatics Studies	Informatics Studies No. 3. Part 1: Report by the Panel on Policy Issues of computer/ telecommunications interaction. Part 2: Report on computers and telecommunications by Dieter Kimbel, Consultant to the OECD.
4	1973	Towards Central Government Computer Policies: Database developments and international dimensions.	OECD Informatics Studies	Informatics Studies No. 5. Consultant's report on the meeting of the Data Bank Panel on 17-18 May, 1972. Panel members included government representatives from Member countries. The panel considered: issues in central government policies for database development to improve efficiency in the public sector; parliamentary and public concern with their social consequences; and the international dimensions of these developments.
5	1974	Automated Information Management in Public Administration	OECD Informatics Studies	Informatics Studies No. 4. Consultant's report highlighting policy issues created by the rapid development of governmental administrative information systems. Part 1: Statement of the Conclusions of the Data Bank Panel (comprising government representatives from Member countries). Part 2: The background report prepared by consultant Klaus Lenk.
6	1974	Applications of computer/ telecommunications systems.	OECD Informatics Studies	Informatics Studies No. 6. Part 1: Statement of conclusions of the Computer Utilisation Group in relation to a survey. Part 2: The evaluation of the performance of computer systems.
7	1974	Information Technology in Local Government: A Survey of the development of urban and regional systems in five European countries.	OECD Informatics Studies	Informatics Studies No. 7. Part 1: The statement of conclusions adopted by the Group of Experts on Information Technology in Urban Management (8-9 March, 1973). Membership included representatives from government government departments of member countries. Part 2: Background report prepared by Paul Kenneth and Claude Maestre, Consultants to the OECD.
8	1975	Applications of computer / telecommunications systems. Proceedings of the OECD Seminar November 13-15, 1972	OECD Informatics Studies	Informatics Studies No. 8. Follow-up to the seminar on Computer/Telecommunications Systems. (Also the subject of Informatics Studies No. 11).
9	1974	Policy Issues in Data Protection and Privacy: Concepts and Perspectives. Proceedings of the OECD Seminar 24th to	OECD Informatics Studies	Informatics Studies No. 10. Proceedings of the seminar on data protection and privacy held at the OECD from June 24-26, 1974. The initiative to hold the seminar came from the Data Bank Panel created by the OECD Computer Utilisation Group to study policy issues arising from the widespread use of computerised data banks.

NO.	YEAR	DOCUMENT TITLE	DOCUMENT TYPE	BACKGROUND
		26th June 1974.		
10	1975	Training Policies for Computer Manpower and Users.	OECD Informatics Studies	Informatics Studies No. 9. Part 1: Statement of Conclusions adopted by the Members of the Group on Training Policy Issues for Computer Manpower Users. Members of the drafting group included government department representatives of member countries and representatives from the University of Southern California and Ecole Supérieure d'électricité. Part 2: Reports submitted at the Seminar on Training Policies for Computer Manpower and Users 21-23 May, Paris 1973).
11	1976	*Conference on Computer/ Telecommunications Policy. Proceedings of the OECD Conference, February 4-6, 1975*	OECD Informatics Studies	Informatics Studies No. 11. Proceedings of the OECD Conference on Computer/ Telecommunications Policy, Paris, February 4-6, 1975. The proceedings contain speeches and background reports. The aims of the conference included "exposing senior government officials to new concepts and emerging policy dimension in the field" and promote international discussion on matters of mutual interest, including the merger of the computing and telecommunications industries, standardisation and minimising social impact (eg. privacy).
12	1980	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: Organisation for Economic Co-operation and Development.	Guidelines.	Guidelines to facilitate the free flow of personal data across national borders in accordance with a global minimum standard of privacy protection.
13	1985	Declaration on Transborder Data Flows	OECD Digital Economy Papers	OECD Digital Economy Papers No. 1 Agreement by member countries to recognise the importance of transborder data flows to their respective economies and to reinforce the importance of the OECD Guidelines.
14	1985	Declaration on Transborder Data Flows	OECD Legal Instruments	Ministerial Agreement signed on 11 April 1985 to promote access to transborder data and services, and avoid unjustified barriers to data exchange. It also aims to seek transparency and consider the impact of actions on other countries.
15	1989	Declaration on the Social Aspects of Technological Change (Abrogated 2016)	OECD Legal Instruments	Recommends policies to stimulate widespread diffusion and exploitation of new technologies. Recommends countries devise more innovative approaches to tackle unemployment and displacement. Recommends the creation of economic and social environments conducive to innovation. States that: "Technological change is necessary to economic and social progress" and therefore workers may slow technological change by resisting it (4).
16	1997	Sacher Report	OECD Digital Economy Papers	OECD Digital Economy Papers No. 29. Report prepared by the Sacher Group of high-level private sector experts on electronic commerce. Companies represented included Marks & Spencer, Barclays Bank,The Bank of Montréal, Nestlé and American Express, among others. Aims of the report included promoting economic growth through e-Commerce and pursuing new government-business partnerships to enable this growth.
17	1998	Dismantling the Barriers to Global Electronic Commerce,	OECD Digital Economy	Digital Economy Papers No. 38 Conference Report. Conference of 400 people, comprising government officials from

NO.	YEAR	DOCUMENT TITLE	DOCUMENT TYPE	BACKGROUND
		Turku (Finland) 19-21 November 1997	Papers	Member and non-Member countries, 14 from NGOs and 130 from business. Aims were to develop principles to enable economic commerce to prosper and to enable private sector "explorers" "on the threshold of the electronic world" to "discover" the extent to which this new world can reap "riches" and further "the magic of the marketplace" (18-20).
18	1998	OECD Ministerial Conference. "A Borderless World: Realising the Potential of Global Electronic Commerce. (Ottawa Conference)	OECD Ministerial Conference	Conference Conclusions. The economic growth potential of e-commerce relies on the removal of impediments to its development. These are primarily posed by government regulation, but also by industry. Proposed principles for a shared global vision of electronic commerce: Competitive; trust for users, such as through government safeguards; legal frameworks "only where necessary" (p. 6); government intervention only when necessary for the "public interest. Encourage self-regulation to avoid government "over-regulation" (p. 9) by taking into account "fundamental public interests, economic and social goals, and working closely with governments and other players" (p. 4-5), privacy protection, voluntary codes, model contract provisions, authentication, and consumer protection.
19	1999	Economic and Social Impact of E-commerce: Preliminary Findings and Research Agenda.	OECD Digital Economy Papers	OECD Digital Economy Papers No. 40 The report focuses on expected effects of e-Commerce on economic growth, economic efficiency, organisational change, employment and broader social issues. E-commerce viewed as part of major societal transformation: the shift towards an economy based on information and knowledge, and increasing prominence of technology in everyday life (p. 18). Concern that E-Commerce benefits may not reach all people and this may create "haves" and "have-nots".
20	1999	Electric Commerce: Initial Survey of Unilateral Liberalisation and Facilitation Measures.	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 45. Survey of unilateral liberalisation (tariff reduction, relaxation of foreign investment restrictions) and facilitation measures (eg. Removal of taxes, provision of subsidies) taken by governments to foster Internet-based commerce.
21	1999	A Global Action Plan for Electronic Commerce: Prepared by Business with Recommendations for Governments.	OECD Digital Economy Papers	OECD Digital Economy Papers No. 44. Report prepared by the Alliance for Global Business. Concerns principles to govern electronic commerce in areas of consumer trust, content and security. Argues that industry regulation is preferable to government regulation due to greater flexibility. Gives responsibility to users/consumers, who are able to exert control over privacy levels through "choice" (20).
22	2000	Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks.	OECD Digital Economy Papers	OECD Digital Economy Papers No. 66. The Report discusses the development of model contracts for transborder data flow contracts and how to ensure effective enforcement mechanisms.
23	2004	Digital Delivery of Business Services	OECD Digital Economy Papers	OECD Digital Economy Papers No. 79. Report prepared by John W. Houghton, Centre for Strategic Economic Studies, Victoria University, Melbourne, Australia in conjunction with the OECD Secretariat, with support from the European Commission. Recommends removal of barriers to enable the digital delivery of business services, which can increase revenue and decrease

NO.	YEAR	DOCUMENT TITLE	DOCUMENT TYPE	BACKGROUND
				costs. Recommends strengthening frameworks for the digital delivery of business services.
24	2006	Future Digital Economy: Digital content creation, distribution and access - Conference Conclusions.	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 118. Conclusions of the Conference on the Future of the Digital Economy in Rome 30-31 January 2006. Representatives from the governments of member countries, universities, the European Commission and industry (eg. Verizon Communications, Google, Yahoo, Confederation of British Industries, IBM, STMicroelectronics, and publishing and music industry representatives).
25	2008	The Seoul Declaration for the Future of the Internet Economy	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 147. Declaration arising from the Ministerial Session. Statement on Ministers' "common desire to promote the Internet Economy and stimulate sustainable economic growth and propensity by means of policy and regulatory environments that support innovation, investment, and competition in the information and communications technology (ICT) sector" (4).
26	2008	Shaping Policies for the Future of the Internet Economy	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 148. OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, Korea, 17-18 June 2008. A report prepared to support the objectives of the Ministerial Meeting, including encouraging the development of the Internet economy.
27	2009	Policy Responses to the Economic Crisis	OECD Digital Economy Papers	OECD Digital Economy Papers No. 159 Report on the impact of the economic crisis and preparation of a strategic response focusing on two policy areas: finance, competition and governance; and restoring long-term growth. Recommends investment in high speed broadband and ICT "to secure economic and social benefits" (13). Recommends linking "ICT investment with other large infrastructure such as roads, buildings, transportation systems, health and electricity grids, which allows them to be "smart" and save energy (eg. "smart grids" (32)], assist ageing infrastructure, improve safety and adapt to new ideas" (13)).
28	2011	The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines.	OECD Digital Economy Papers	OECD Digital Economy Papers No. 176. Report on the development and influence of the Guidelines, as well as the current landscape of privacy policy, with an economic focus. Report prepared by Barbara Bucknell, Office of the Privacy Commissioner of Canada.
29	2012	Laying the Foundation for the Internet Economy: Access to the Internet via a High-Speed Infrastructure.	OECD Digital Economy Papers	OECD Digital Economy Papers No. 201. A Review of the Seoul Declaration by the Committee for Information, Computer and Communications Policy (ICCP). Presents developments in the Internet economy since the Seoul Declaration, to report on progress and flag new issues.
30	2013	Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines	OECD Digital Economy Papers	OECD Digital Economy Papers No. 229 Proposed revisions to the OECD Privacy Guidelines (1980) to call upon member countries to "consider the role of actors other than data controllers, in a manner appropriate to their individual role" (9). The provision intends to make policymakers aware of individual actors (9). Proposed the possibility of revising the data collection limitation principle to be more precise to account for increasing capacity for its "valuable re-use" for example in the 'public interest' (9-11). Discussion about giving responsibility to individuals, such as

NO.	YEAR	DOCUMENT TITLE	DOCUMENT TYPE	BACKGROUND
				through education about privacy risks and gaining their consent (6).
31	2013	The App Economy	OECD Digital Economy Papers	OECD Digital Economy Papers No. 230 Report prepared by the Working Party on Information Economy in the context of the OECD's work on digital content. Purpose to inform about the "app economy" in the interest of minimising barriers to continued development of the app economy, which has shown "spectacular growth" during the economic downturn (5). Issues identified for consumers include contract clarity, complexity of the legal landscape, misleading or unfair commercial practices and privacy (37). Barriers to adoption of apps should be reduced.
32	2015	Industry Self Regulation: Role and Use in Supporting Consumer Interests	OECD Digital Economy Papers No. 247.	OECD Digital Economy Papers No. 247. Report prepared by the Committee on Consumer Policy to examine the role that industry self-regulation can play in addressing consumer issues, such as Advertising codes and 'trustmarks' (5).
33	2015	Data-Driven Innovation: Big Data for Growth and Well-Being	Report	Report seeks to seize the benefits of data-driven innovation and the datafication of the economy which are part of the "pivot to a data-driven world".
34	2016	Economic and Social Benefits of Internet Openness	2016 Ministerial Meeting on the Digital Economy.	Background Report. Prepared as background for a discussion at the OECD Ministerial meeting on the Digital Economy, 21-23 June 2016 in Cancún, Mexico. It presents a framework for understanding and analysis of Internet openness. Proposes "balanced" approaches to "protecting competition, consumers and privacy" on the Internet in order to preserve internet openness (technical, economic and social openness) (8). Internet openness is viewed as necessary for economic growth, social well-being, international trade, innovation and macroeconomic performance (5,8,14).
35	2016	Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration)	OECD Legal Instruments	The Cancún Declaration calls on governments to actively leverage the opportunities of the digital economy for more sustainable and inclusive growth focused on well-being, equalities of opportunities, and trust.
36	2018	Consumer Product Safety in the Internet of Things	OECD Digital Economy Papers	OECD Digital Economy Papers No. 267. The report was developed by the OECD Working Party on Consumer Product Safety as a follow-up to its work on online product safety and as a companion to the work by the Committee on Consumer Policy on Consumer Policy in the Smart Home. The report was prepared by Rod Freeman, international product safety lawyer and partner at Cooley (UK). The report addresses the consumer product safety benefits and challenges raised by the Internet of things.
37	2018	Consumer Policy and the Smart Home	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 268. Report prepared by independent consultant Richard Bates outlining the key consumer benefits and risks associated with Internet of Things (IoT) devices in the "smart home". Concerned with questions such as "What does ubiquitous but invisible data collection by smart home devices mean for traditional approaches to protection of personal data, and how can transparency be ensured?" (5). Privacy and consumer risks of "smart" devices need to be mitigated in order to maximise the benefits of ubiquitous and "invisible" monitoring by devices which are "continually listening or observing" (4).

NO.	YEAR	DOCUMENT TITLE	DOCUMENT TYPE	BACKGROUND
				Surveillance (monitoring and data collection by sensors) is necessary for convenience, customisation, energy efficiency, safety and control (4).
38	2018	Improving online Disclosures with Behavioural Insights	OECD Digital Economy Papers	OECD Digital Economy No. 269. A report from the Committee on Consumer Policy about how to incorporate "behavioural insights" ie. "findings from economics, psychology, neuroscience and marketing to better understand how individuals and businesses actually behave in the marketplace." The report looks at how behavioural insights can be used to improve online information disclosures for consumers.
39	2018	AI: Intelligent Machines, Smart Policies	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 270. Conference Summary. Conference held in Paris, 26-27 October 2017 and was sponsored by the Japanese Ministry of Internal Affairs and Communications (MIC). Delegates included policymakers, representatives of civil society and AI experts from industry and academia. Interactive demonstrations were provided by Google Arts & Culture and Facebook.
40	2019	Online Advertising: Trends, Benefits and Risks for Consumers	OECD Digital Policy Papers.	OECD Digital Policy Papers No. 272. Report prepared by the OECD Secretariat. Introduces key aspects of online advertising and outlines the main benefits and risks for consumers.
41	2019	Vectors of Digital Transformation	OECD Digital Policy Papers	OECD Digital Policy Papers No. 273. Report on the ways digital transformation challenges existing policies.
42	2019	Enhancing the Contribution of Digitalisation to the Smart Cities of the Future	OECD Paper.	Paper produced by the OECD's Centre for Entrepreneurship, SMEs, Regions and Cities. Recommends the development of a "Smart City Measurement Framework" to measure smart city performance, ie. "to measure the "smartness" of the city" (12). Implement policies to boost the "well-being" of citizens and include well-being indicators in the Measurement Framework.
43	2019	Artificial Intelligence in Society	Book.	The book builds on the 2017 conference on "AI: Intelligent Machines, Smart Policies". The book maps the economic and social impacts of AI technologies and applications and their policy implications, presenting evidence and policy options.
44	2019	Recommendation of the Council on Artificial Intelligence ('AI Principles')	OECD Legal Instruments	The recommendation aims to foster innovation and trust in AI by promoting the responsible stewardship of AI whilst ensuring respect for human rights and democratic values. Recommendations to national policy-makers (3): 1. Invest in AI research and development. 2. Foster a digital ecosystem for AI. 3. Shape an enabling policy environment for AI. 4. Build human capacity and prepare for labour market transformation. 5. Build capacity for international co-operation for trustworthy AI. Promote the use of AI for Covid-19 recovery, such as through Google's Community Mobility Reports (5).

NO.	YEAR	DOCUMENT TITLE	DOCUMENT TYPE	BACKGROUND
45	2019	Going Digital: Shaping Policies, Improving Lives	OECD Report.	A Report prepared by the OECD Secretariat on the ongoing "digital transformation".
46	2020	Smart Cities and Inclusive Growth: Building on the Outcomes of the 1st OECD Roundtable on Smart Cities and Inclusive Growth.	OECD Policy Papers.	Summary of discussions held during the 1st OECD Roundtable on Smart Cities and Inclusive Growth (9 July 2019, OECD Headquarters, Paris, France) as well as additional research.
47	2020	2nd OECD Roundtable on Smart Cities and Inclusive Growth: Preliminary Agenda.	Meeting Agenda.	Items on the Agenda include: Redefining the concept of smart cities to "deliver concrete well-being outcomes for all people" (2); and Develop instruments to measure well-being outcomes (2).
48	2020	Using artificial intelligence to help combat COVID-19.	Tackling Coronavirus (COVID-19): Contributing to a Global Effort.	Briefing paper on AI and its use in responding to COVID-19. Part of the OECD's work in relation to the pandemic: oecd-org/coronavirus.
49	2021	The Effects of Online Disclosure About Personalised Pricing on Consumers: Results from a Lab Experiment in Ireland and Chile	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 303. The Report was prepared by the Economic and Social Research Group. Results of experiments in Ireland and Chile to test the consumer impact of online disclosures on personalised pricing.
50	2021	State of Implementation of the OECD AI Principles: Insights from National AI Policies	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 311. The report was developed by the working group on national AI policies of the OECD.AI Network of experts, which comprises industry representatives, civil servants from member countries and independent organisations, such as The Future Society, working with AI governance issues.
51	2021	Tools for Trustworthy AI: A Framework to Compare Implementation Tools for Trustworthy AI Systems.	OECD Digital Economy Papers.	OECD Digital Economy Papers No. 312. Presents the work conducted by the OECD Network of Experts on AI (ONE.AI) working group on implementing Trustworthy AI to develop a framework for comparing tools and practices to implement trustworthy AI systems, as requested by the Committee on Digital Economic Policy. The list of 94 Members and observers includes representatives from member countries, industry (including Google, Facebook, EY AI Lab, AT&T Labs, IBM, Microsoft, Inter-American Development Bank, Emerj AI Research, Thales, Sanofi), independent experts and policy consultancy organisations.
52	2021	Recommendation of the Council on Enhancing Access to and Sharing of Data.	OECD Legal Instruments	Sets out general principles on and policy guidance on how governments can maximise the benefits of enhancing data access and sharing arrangements whole protecting individuals' and organisations' rights and taking into account other legitimate interests and objectives.
53	2022	OECD Framework for the Classification of AI Systems	OECD Digital Economy Papers	OECD Digital Economy Papers No. 323. Report prepared by the OECD Secretariat. Aims to assist policy makers, regulators and others characterise AI systems with a tool to to evaluate AI systems from a policy perspective (3). The framework aims to guide "an innovative and trustworthy approach to AI as outlined in the OECD AI principles" (3).

Published by
Alexander von Humboldt Institute for Internet and Society

in cooperation with
CREATe
cnrs centre internet et societe
R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya
University of Tartu Johan Skytte Institute of Political Studies