Integrity and security discourses in three European countries' AI policies.

A study in privacy, political theory and rapidly developing technology.

By: Bror Åhammar

Supervisor: Fredrika Björklund
Södertörns Höhskola – Institution for Political Science
Master Thesis VT 2022
Political Science
**Table of Contents:**

Abstract 3

1. Structure: 3
   1. 1. Background 3
   1. 2 Research questions, basic outline and purpose 4
   1. 3 Definition of privacy 6
   1. 4. GDPR as an example of privacy regulation and overarching framework 7

2. Theory: 8
   2. 1. Björklund and Zuboff's contributions as theory 10
   2. 2. Discourse analysis as theory 11
   2. 3. New Public Management theory 12

3. Methodology: 12
   3. 1. Operationalization 14
   3. 2. Validity and reliability 14

4. Previous research: 15

5. Material: 17
   5. 1. The countries' history with AI and privacy 18
   5. 2. The countries' strategies 19
   5. 3. Laws, torts and other governmental documents 20
   5. 4. News articles 21

6. Analysis: 22
   6. 1. United Kingdom 22
   6. 2. Sweden 27
   6. 3. Estonia 32
   6. 4. Comparing strategies 40

7. Conclusions: 43

Sources 43
Abstract:

The relatively recent developments in AI have caused a lot of discussions surrounding security and privacy, and a consistent theme throughout these discussions have been how privacy as a political and legal term have developed in response.

While this isn't necessarily a new phenomenon – privacy concerns have been around since the 19th century when Warren and Brandeis published their seminal paper – the development of AI has marked a new period where privacy has become a socio-political issue. The development of AI also have happened concurrently with changes in governmental paradigms, which makes this relevant albeit possibly difficult to interpret. That makes communicative events – the AI strategies, privacy regulations and news articles – important empirical material for the study.

The study's main purpose will be to study how three selected countries - and the practices within them – have shaped their respective artificial intelligence strategies through privacy regulations. This is an important question to ask when changes in organizational ideology have occurred and resulted in New Public Management – an ideology more friendly towards corporations than its 1950s-70s predecessor, when AI was in its infancy.

For the purpose of this paper the term artificial intelligence will refer to computer programs and systems on the software level; they are interently dealing with data as a part of their function. And the computer does not check the security and privacy-related implications for the data use unless the programmer specifically makes the artificial intelligence do so; and there are many cases where that would be difficult.

The countries chosen for the paper – the United Kingdom, Sweden and Estonia – were selected partly because they are democratic countries, but also partly due to their different stances on artificial intelligence, history and governance methods. These three do share some unifying aspects, such as all being European countries and signatories of the EU's GDPR treaty.

The resulting comparision illustrates that differences between the three countries' existing practices do affect how AI strategies and regulations are formed – an important consideration in an environment where privacy has become an intense topic of debate.

Keywords: Artificial intelligence, New Public Mangement, practices: political-parliamentary, juridical-bureaucratic, public, countries' strategies, GDPR, communicative events.

1. Structure:

1.1. Background and research problem:

The IBM's System/360 from the 1960s is a notable milestone in the early development of artificial intelligence - AI. One of the examples became the ”Martinsburg Monster” when it was bought by the American IRS in 1965; and its source code was the basis of the IRS' tax return system until it failed on Tax Day in 2018 (Taxpayer Advocate Service 2020, p. VI). It already showed some integration of artificial intelligence into every-day governance procedures: at the point it was purchased the IRS struggled to keep up with the number of tax forms they were handling each Tax Day.

While privacy had become an important topic of debate beforehand – such as Warren and Brandeis'
seminal paper published in 1890 – computers like the Martinsburg Monster marked a major inflection point since they could process information quickly as the government wanted. The CBS reporter covering this story – Harry Reasoner – noted in 1970:

"There are those at Internal Revenue who say that if this building in Martinsburg, West Virginia, were filled with hay instead of computers, it still would put the fear of God in us all, so long as it said 'National Computer Center' on the outside.” (Reasoner 1970)

The fact that such a relatively simple artificial intelligence could arouse a lot of discussions regarding personal integrity and security raises an important point in regards to artificial intelligence; with the continued advancement of computing technology, artificial intelligence's capabilities and their integration into both state structures and wider society, it is certainly plausible that these discussions have become much more widespread since the days of the Martinsburg Monster – both within parliaments, juridical systems and amongst the public. The Martinsburg Monster example hints at disquiet coming from the public, although it is not necessarily confined to that sector alone – discontent can be voiced through direct content of the speech being used as a restraint, or the indirect relationship between parties. And where there's disquiet there will likely be action taken in response.

These implicit developments do not happen in a vacuum either – they're accompanied by prominent changes to organizational theory, such as the emergence of the market-focused New Public Management (NPM) paradigm over the bueracratic-focused paradigm predominant in the 1970s. NPM is important to this study since the changes in government paradigms affect how parliaments, juridical systems and the public will percieve the associated privacy issues.

If people do not know how parliaments, juridical branches and the public interact with AI and how privacy-related regulations affect AI strategies – or to which extent the countries lean on market-focused solutions or the EU's GDPR - then faith in those regulations and strategies will inevitably be undermined. This has significant implications for how countries plan their AI strategies, since AI strategies will thus have to account for privacy regulations in turn lest they undermine faith in those regulations.

There is also a notable research gap here – not many papers or books have looked into how countries diverge when it comes to these regulations, and this creates a need to study these differences in further detail.

This can be seen by picking three countries for this study – the United Kingdom (treated as synonymous with Britain for the purpose of simplicity), Sweden and Estonia – and in particular studying how their respective parliaments, juridical systems and public act and react in response to these privacy-related quandaries.

1.2 Basic outline, purpose and research questions:

The basic outline of this paper will primarily focus on adressing the research problem by analyzing the data – defined as the three selected countries and their AI strategies. The paper will as such rely on previous research: the studies by Björklund and Zuboff in to video surveillance.

The paper will utilize Björklund's definitions of practices – the political-parliamentary, the juridical-bueracratric and the public - as the basis of its theory: that the various practices within those three countries represent power structures independent from each other, and that said power structures
can use methods of soft power to influence not just other practices but also nongovernmental organizations like corporations.

The paper defines “power structures” as structures relatively independent from each other and are represented by a body capable of exercising power within the country's political system. By calling practices “power structures” the paper raise the implication that one practice in a country will often interact with the other two practices in the same country – not necessarily in an equal relationship. This power can - according to Fairclough - be exercised either through the contents of the discourse, the relations between the power structures, and the positions they subsequently take. Thus power structures can use power in discourse to restrain each other. (Fairclough 2013 p. 14)

The parliamentary practice is represented by the country's parliamentary body, whose primary power and decision-making is made through the legalisation of laws. The juridical-bureaucratic practice is represented by the the justice system and the bueracracy, whose implementation of laws and torts can often serve as legal and organizational precedence for other practices to follow. And the public practice is represented by the public itself, whose decision-making is more informal and primarily through citizens interacting with politicians and judges. (Björklund 2013 p. 26)

Thus the practices build and maintain privacy laws and enforce them. The definitions of communicative events and soft power will primarily be drawn from Fairclough's critical discourse analysis – particularly his definition of power through the use of constraints imposed from one practice.

The decision to use the terms “communicative events” and “power” in a study focused around privacy might seem completely contradictory to the purpose of privacy. But it is justified on the same grounds as Warren and Brandeis pointed out in their defining work on privacy: this is a field where if privacy legislation is not established or enforced then more malevolent individuals and organizations can hypothetically run rampant with peoples' information without consent. (Warren and Brandeis 1890).

The primary purpose of this study is to answer how the practices act and interact when it comes to privacy regulations. The aim of the resulting comparison is to illustrate how the countries' privacy regulations and AI strategies diverge; which is of further interest considering the three countries used to share the same basic privacy regulation – the EU's GDPR.

With that in mind the analysis' structure will focus on the three specifically chosen countries. These countries – Britain, Sweden and Estonia - are chosen due to their different socio-political structures and their respective established political-parliamentary and juridical-bureaucratic, and public practices prior to the emergence of AI.

The theoretical and methodological tools used come from two books: Björklund's “Video surveillance in theory and as Institutional Practice” and Zuboff's “Age of Surveillance Capitalism”. This is to prove that their research into video surveillance can be applied on the more general field that AI represents.

The EU is of significant interest here: all three of the countries are or were members - until recently, when UK exited in the much publiced Brexit referendum and subsequent withdrawal process. Still, Sweden and Estonia both remain within the EU as well as its legal and regulatory framework. This is very important for the study since the framework provides a rather interesting contrast between the UK on one side of the coin; and Sweden / Estonia on the other. It is for that reason that the EU's
landmark legislation GDPR is included in this study, as a comparative tool akin to NPM.

On that note, that contrast is one reason why these three countries are chosen. They are also chosen for their different structures: both politically and vis-a-vis security / privacy. These differences are assumed not just due to their different demographics or histories, but also due to a different political systems and basis for privacy regulations.

The UK has a long history of tort law determining privacy-related matters - which extends back to at least the 1970s, as Wainwright v. Home Office alluded to by referring to previous privacy-related tort cases (Wainwright v. Home Office 2003).

Sweden is presumed to have an entirely different starting point since that country has not had the same history with tort laws; instead the paper will work with the assumption that the Swedish position is primarily determined by laws coming from the political-parliamentary process (Riksdagen 2004:51).

Estonia is a case where the state has long had a major say in shaping not only computer development – although that was of an authoritarian character. Thusly, this paper will work with the presumption that Estonian developments in AI and privacy come as a reaction to – and effort to distance itself from – its Soviet dominated past.

That brings up this paper's main research questions:

How do the countries studied – Britain, Sweden and Estonia - and their AI strategies diverge, and how do privacy legislation contribute to that divergence? How much are the respective countries' strategies affected by New Public Management and the EU’s GDPR?

To help discern these differences it is worth asking: how do the studied countries' political-parliamentary, juridical-bureaucratic and public practices respectively interact with each other when it comes to AI and privacy? Is one of the practices the primary decision-making arena? And is the power primarily exercised through the content of the discourse, or through relations and subjects?

1. 3. Definition of privacy:

The study's definition of "privacy" will chiefly be from Samuel Warren and Louis Brandeis' "The Right to Privacy" which chiefly concerned itself with photographs and newspapers raising new privacy-related questions.

Warren and Brandeis conceived of privacy as a political and legal matter mainly “The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others . . . fix[ing] the limits of the publicity which shall be given them.” (Warren and Brandeis 1890 p. 198, via Glancy, Dorothy J 1979 p. 2) They make direct references to "the common law" which further implies an already existing law – Glancy noted:

"Warren and Brandeis deliberately concluded their article with the powerful image of the common law right to privacy in the hands of the embattled individual as an age-old weapon “forged in the slow fire of the centuries, and to-day fitly tempered to his hand.” (ibid, p. 220, via Glancy p.3).

The notion of privacy being primarily developed within the American political and legal system has
significant implications for the study: especially since both the British and the Swedish artificial intelligence programs were heavily influenced by American efforts. The work by Alan Turing and his colleagues occurred while America directly assisted Britain during World War 2 and the post-war, while Swedish interest in artificial intelligence surfaced in the post-war era and directly borrowed from the American developments. (Hallberg 2007 p. 127-131)

1.4. GDPR as an example of privacy regulation and overarching framework:

For the purpose of this study the EU's General Data Protection Regulation – introduced in 2016 under the article number 2016:679 and hereby referred to as GDPR – is going to be used as a prototypical privacy regulation and as an comparative case study: the three AI strategies are going to be affected by the GDPR by virtue of all three countries having long-standing relationships with the EU, but the question is to which extent.

Since the GDPR is aimed to be unifying framework it is not just all-encompassing but also intended to be comprehensive. This is evident already in the second paragraph:

"The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons."

This paragraph does not address privacy immediately, however it makes a direct reference to the protection of personal data, which in turn can be seen as equivalent with privacy. Security is here grouped together with freedom and justice, meaning that the GDPR does not consider security as an isolated matter: rather it is intertwined with the presumed notion that security does not undermine freedom or justice.

This is further reinforced by the sixth and seventh paragraphs, with the sixth opening thusly:

"Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.” (European Union 2016/679§ 6)

The sixth paragraph acknowledges the technological developments that have occurred. It also implicitly states that individual people making that data available should be accompanied by protection of peoples' data. The seventh paragraph continues:

"Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.” (ibid § 7)
As a result of this the GDPR sets out to establish and entrench a common data protection framework – particularly since the view that natural persons (which is presumed to be the same as ordinary citizens) should have control of their own personal data is essential to the fulfillment of this law.

The GDPR – as an overarching framework – is establishing the content constraint through the wording of the law. This constraint is flexible, however, as evidenced by the eigth paragraph:

"Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law." (ibid § 8)

There is an argument to be made here that the GDPR will inevitably get interpreted in different situations and in different contexts, so the eight paragraph works as a safeguard. The eight paragraph also allows for interesting divergences, which is the main reason why the study incorporates the GDPR. All three of the studied countries have a long-standing relationship with the EU, and are unavoidably affected by the GDPR as a result.

Even Britain - which was in the midst of the Brexit process when the GDPR was adopted – adopted a form of GDPR called the Data Protection Act. In turn it makes GDPR a major background element, and one that the Data Protection Act directly references:

“For the purposes of the GDPR, the following (and only the following) are “public authorities” and “public bodies” under the law of the United Kingdom:” (Data Protection Act 2018 §7.1)

Since the above paragraph – created in a country that was in the midst of leaving the EU – directly references the GDPR it thus follows that Sweden and Estonia would also be heavily affected by it.

2. Theory:

The main theoretical framework for the study is created through inductive reasoning: that the Björklund's practices of policy discourse - political-parliamentary, juridical-bureaucratic and the public - also are concrete factions chiefly represented by specific institutions or elements of society. Thus they can affect different countries' privacy and AI policies to different degrees and through different discourse methods. Existing theoretical concepts like discourse practice and New Public Management theory will be used to help construct the theory.

The reasoning for this creation of new theory through inductive reasoning is because the intersection between privacy and AI – specifically by practices using communicative events to implement and influence new regulations or otherwise change - is relatively under-explored.

In this case, the inference is that practices being active factions would explain how they react to situations similar to that of the Martinsburg Monster creating a public stir. In that case it was the public practice represented by the public that. And thus how the practices create, reform and maintain privacy-related laws and regulations and take AI-related events into account. Another inference then is that a critical discourse analysis would help to explain the process since most of the material involved are documents – whether official documents or news articles.
The central limitation to this theory is that since it is inductive it inevitably runs into the practical reasoning dilemma. (Ketokivi & Mantere 2010 p. 315) Since practical reasoning proceeds from various grounds to various claims in order to convince the audience – in this instance, the existence of practices leads into the inference that those practices are active factions – it also leads to the acknowledgement that there are no universally accepted principles to govern the practical reasoning process. In particular, inductive reasoning lacks the normative foundation that deductive reasoning has, and is thus methodologically incomplete.

However, inductive approaches are very well-suited towards cases where studies attempt to discover new insights through in-depth case studies and ample data collection (Wodak & Meyer 2009 p. 19). This is something the study aims to do – particularly since the material chosen ranges from official documents to news articles. So an inductive approach is chosen instead of a deductive approach, which focuses on a closed theoretical framework and illustrate the assumptions with a few examples.

As such, this paper seeks to explore using the inference to the best explanation, which ideally assumes that the researcher selects the best suited theory to explain certain phenomena. (Ketokivi & Mantere 2010 p. 319) “Inference to the best explanation” seeks to alliviate the practical reasoning dilemma by contextualizing the reasoning behind why an inductive strategy is chosen.

The alliance between inductive reasoning and critical discourse analysis is a very uneasy one, and in an effort to alliviate the practical reasoning dilemma this study will use a contextualization strategy, which assumes that the inference and the explanation are the same. (ibid p. 320) “Inference to the best explanation” showcases that there is no holy grail amongst theoretical approaches – but inferences can study the practices' actions and help uncover how they create and maintain privacy regulations and incorporate AI into those regulations.

Another limitation of the theory is that by considering the practices separate the theory might not fully account for instances where they cooperate or function in symbiosis. For instance, the political-parliamentary and juridical-bureaucratic practices are implicatedly intertwined to some degree since the former usually enshrines new laws while the latter enforces them via bureaucratic processes.

These are primarily made to distinguish different areas of socio-political activities, although it is worth noting that these terms are also meant to emphasise how different countries tackle them. Within that context one limitation of this division does show: the three practices do not account for economic motives. While this is not necessarily a major concern in itself, it is still worth noting since this paper deals with corporations who may not interact with these practices in a manner entirely consistent with these definitions.

The theory will also assume that the practices in turn influence security and privacy-related policies – as well as legal developments like tort laws. In turn these tort laws influence the AI strategies, creating an indirect cause-and-effect.

This study will primarily use a critical discourse analysis as a conduit for the theory. This is mainly because domestic political actors and their actions is treated as the actors causing change for the purpose of this paper, although it also highlights the regulatory aspects involved. In addition, the cause-and-effect relationship also puts language in a primary position, which is one main reason critical discourse analysis will be used. The practices use language to exert power and enact change.
in both legislation and policies like strategies, after all.

2. 1. Björklund and Zuboff's contributions as theory:

The paper will use Björklund's chapter “Video surveillance in theory and as Institutional Practice” in the book “Video Surveillance and Social Control in a Comparative Perspective”. as well as Susanna Zuboff's “The Age of Surveillance Capitalism” as primary theoretical and methodological tools. Björklund's definitions of practices

Björklund discusses video surveillance from the point of view that emphasises the political and legal aspects, but also their public effects. This is noted by them coining the terms "political-parliamentary”, "juridical-bureaucratic” and "public” to describe the different avenues through which developments in video surveillance takes.

Zuboff takes a much different view, and works primarily with Google and the neoliberal consensus of the late 90s up to 2010 as the primary forces favoring megacorporations such as Google. (Zuboff p. 75) Unlike Björklund she therefore takes a much more critical stance on megacorporations' aspirations and goals; in particular, she deems one of the foundations of surveillance capitalism as an all-consuming desire for more data. (ibid p. 88)

Zuboff's conclusion is rather damning on surveillance capitalism because she views surveillance capitalists' pursuits as departing from long-standing organic reciprocities with people while also demanding unfettered freedom and knowledge – including the ability to expand on that knowledge if neccessary.

Björklund highlighted, however, that video surveillance - itself an possible extension of both digitalization and artificial intelligence since surveillance tools like cameras oftentimes are digital cameras that run on AI programs – have been posited as social seperation and exclusion issue. (Björklund 2013 p. 22).

Zuboff's interpretation does differ from Björklund's to a significant degree, though, especially since the issue of extraction is central to her interpretation. From her perspective the enshrinning of data as a fundamental right is an attempt to constrain the advance of surveillance capitalism, and not one that is guaranteed to succeed since the surveillance capitalists have a vested self-interest in retaining control.

With that in mind the comparision between Björklund and Zuboff does have some merits in this context: particularly when framing the discussion surrounding the GDPR. Björklund's interpretation may be better suited for situations where the dividing lines between the different processes are more clear cut, while Zuboff's view may be better suited for instances when the difference between state and corporation is not as evident,

This does make it a bit more difficult to view specific interactions from a relations or subject perspective, however, and might make it more difficult to distinguish between practices. For that reason, Björklund's interpretation of discourse may be more easily analyzed in these cases: because she presents clear cases of conflicting interest.

However, Zuboff's interpretation might be more suited to situations where the contents is the main constraint: since the content restriction is primarily about what is said or done. So in instances where the government clearly acts against a non-governmental actor such as a corporation Zuboff's
view becomes. For instance, the definition of security and privacy can overlap to some degree when it specifically comes to AI and computer software: after all, misuse and theft of personal data is both a security and privacy issue.

2.2. Discourse analysis as theory:

The theory does lean to some extent on the idea of the practices as governance structures also maintain different discourse methods. Discourse practice is defined by Fairclough as not only a part of Critical Discourse Analysis (CDA), but also a form of “social practice” where discourse is effectively shaped by relations of power and ideology but can also be used itself to entrench those relations. (Fairclough 2013 p. 10)

Because discourse practice is dependent on the idea that language creates points of view, discourse practice thus has a constructivistic outlook on how reality is shaped. (Winther Jørgensen & Phillips 2000 p. 9) Discourse theory is not necessarily limited by one approach, but all approaches hold that language is reality-creating; in that the language used has different applications of values, which in itself build connections and meaning. (Bergström & Borèus, 2012, p 353)

In that sense, the connection between privacy regulations and AI are themselves created by the language used. The Martinsburg Monster example is a case in point: AI is deployed in governmental organizations to examine tax records without people knowing. When people find out about the Monster, they panic – thus the public practice helps to create the reality that the implementation of AI without peoples' knowledge is dangerous and exercising discursive power that way

Björklund alludes to the idea that the practices can be seen as representing the respective political arenas, the people within those arenas as well as the respective discourses occurring within those arenas. (Björklund 2013 p. 31)

For instance, while the political-parliamentary practice and juridical-bureacratric practice refer to formal practices, the political-parliamentary is exercised in arenas where political decisions are made – such as parliaments – as well as politicians; while the juridical-bureacratic practice is mainly centered around juridical review, takes place within the justice system and are going to represent the judges and bueracrats working within said practice. The primary distinction between the political-parliamentary and juridical-bueracratric practices is that the political-parliamentary practice generally enact laws, while the juridical-bueracratric enforce them.

Meanwhile, the public practice is primarily outside of governmental functions and instead defined as what happens in public for a and the public themselves, such as meetings between politicians and the public. The public can still influence laws by their activities – not just voting, but also political activity from below. (ibid p. 37)

As such this paper's theoreical structure is meant to concreticize the processes and different practices into more measurable aspects of governance. By doing that this paper attempts to solve the research problem and questions by applying them to areas where they have not seen as much study: not just video surveillance, but also AI in general. The theory will thus assume that each country's practices – by acting as active factions – react differently to AI's security and privacy-related issues.
2.3. New Public Management theory:

Since the focus will be on governance – particularly within the political-parliamentary and juridical-bureaucratic contexts – this paper will utilize New Public Management (or NPM) as an example of a governance paradigm and as a benchmark. The three cases chosen are likely influenced by NPM to a greater or lesser extent, so the paper aims to study how much NPM discourse has affected the countries in question.

NPM as a governance paradigm fuels a perceived need to change governance structures to corporate interests – it promises to tailor governance according to corporate role models and solve many of the perceived problems that more traditional governance structures had struggled with. (Löfgren 2019 p.1).

While governments can rely on taxes and thus do not need to tailor AI development to an income stream they still have a particular self-interest in making sure that AI are effectively used. Governments usually rely on bureaucracies, and AI at least promises to simplify a lot of the work needed here: Löfgren in particular defined “ICT as NPM” as a management system that focuses on using computing technology to augment an NPM-centric governance structure. (ibid)

While correlation does not imply causation, it is worth noting that it was during the period where NPM was established as a paradigm – the 1980s-90s - that corporations such as Apple, Microsoft and Google became increasingly prominent within the field of computer and AI development. Zuboff refers to these corporations as “surveillance capitalists” and as destructive forces – thus, an NPM-centric government seeking to cooperate with or otherwise emulate these corporations can be perceived as a double edged sword. (Zuboff 2019 p. 14)

The theoretical value of NPM in this paper is that it helps to clarify the differences between the governments that cooperate heavily with non-governmental organizations and actors – which itself changes the bureaucratic system - and the governments that don't rely as heavily on NPM: thus, cases where the government is influenced by NPM are presumed to contrast with cases where the government is not.

There is a risk with overestimating NPM's importance, however. This is most visible in Löfgren's assessment of NPM: its adherents had overestimated the positive effects that NPM has caused while at the same time highlighting that NPM has inadvertently lead to more administrative busywork. (ibid) His argument effectively pressuposes that those in favor of NPM have put the cart before the horse in a certain sense: especially when it comes to whether digitalization has created new opportunities.

3. Methodology:

The methodology will be mainly qualitative, and survey the material – strategy documents, legal documents as well as news articles – by applying a critical discourse analysis. This decision is taken partly because of the theoretical framework being an inductive strategy: inductive reasoning relies a lot on observation, and by surveying the material in question the study intends to generate new conclusions.

The decision to perform a qualitative analysis is also justified on the grounds that the study anticipates significant divergence of thought between the countries. One country like Britain may be
primarily influenced by a specific practice, and countries like Sweden and Estonia might be primarily affected by other practices in their privacy regulations.

The discourse analysis will be based around Fairclough's definition: which defines discourse as “language as social practice determined by social structures” (Fairclough 2013 p. 14). This is done through Fairclough's subdivision of social practice, discursive practice and text respectively.

Fairclough also ties critical discourse analysis to power and ideology respectively – although it is worth noting that the practices' primacy as a discursive practice does not necessarily mean that power is used. While power usage is one method through which discursive practice can enact change, Fairclough also emphasises that discursive practice is primarily social, taking place in distinct institutions (Winther Jørgensen – Phillips, 2000 p. 71 ).

The main focus of the study will thus be on the communicative events in question – that is the instances where the different practices use communication in order to affect the AI strategies whether directly or indirectly.

While “power” will take a secondary position to the communicative events themselves, this term will be used to exemplify one method in which the factions enact change. Fairclough's definition of power subdivides it into power in discourse, and power behind discourse. For the sake of simplicity – and the cause-and-effect mentioned previously - the study will use power in discourse to complement the communicative event in itself.

Power in discourse is primarily the ability by powerful participants to control the conversation and constrain the contributions of non-powerful participants (Fairclough 2013 p. 38) In particular, three constraints are:

* contents, on what is said or done;
* relations, the social relations people enter into in discourse;
* subjects, or the 'subject positions' people can occupy.

Fairclough notes that the three are closely intertwined - although he believes it is still worthwhile to separate them. He separates them via distinguishing their respective linguistic forms and functions – contents is primarily defined as the act itself, relations is describing the social aspect of power in a relationship while subjects encapsulates the position itself.

One country might primarily influence its AI-related policy decisions through a content-specific approach, another may instead lean moreso on the relations and subjects to influence the privacy regulations and AI strategies.

In addition, one of the three practices may have a more central position within one of the three countries while being in a less relevant position in another. As such critical discourse analysis can offer an explanation for certain practices' primacy within the states' privacy policies and AI strategies. (ibid p. 39)

The critical discourse analysis will mainly be applied on a meso (middle) scale: the other dimensions are intentionally excluded since those levels might not contribute directly to determining which practices have a primary influence.
By utilizing a critical discourse analysis the paper aims to clarify the categorisation and help to illustrate how the relatively independent practices influence each country's AI policies – tying the methodology together with the theory.

3.1. Operationalization:

The study's operationalization will primarily survey the material to emphasize which practice is using communicative instances. For instance, if a specific practice in a specific country has helped to shape privacy regulations in that country then it will be noted. And with that established any possible effects that the privacy regulations have on the AI strategy will be noted. Any evidence of the word “privacy” or similar words being used in the AI strategy will most likely indirectly hint at privacy regulation having an effect on the AI strategy in question.

This is the primary inductive approach made by this study, but it is leaning on a couple notions: First, since AI strategies inevitably deal with data management a safe assumption can be made that AI strategies will have to address privacy-related issues. Second, AI strategies would not want to cast the concept “privacy” in a negative light. Any hypotheoretical AI strategy doing so would intuitively incur severe backlash. An AI strategy could hypotheoretically argue that privacy regulations might be too strict, but an AI strategy arguing against the concept would draw the ire of many different instances such as the EU’s GDPR.

It does not exclude the possibility of there being no mention of the word “privacy” in an AI strategy. In any such case a secondary document will be used and studied to see if the absence of the word “privacy” had an effect that the secondary document noted. In order to avoid after-rationalizations and other related problems the study will only draw secondary documents from the same institution that produced the AI strategy, and the secondary documents will only be drawn from timeframe as the AI strategy itself was published. This is important since it reduces the risk that individuals within the strategy-creating institution – or powerbrokers – from changing the circumstances surrounding the AI strategy. Whether from forgetfulness or intent to make an AI strategy look better in retrospect.

This study will also try to discern how much of an effect NPM and the EU's GDPR have on the AI strategies. For those purposes this strategy will look for “growth” as in economic growth to symbolize NPM-centric approaches, and any references to the EU's GDPR will be also noted in a similar manner.

Those two are decisively secondary – and to a large extent external - factors, but they are chosen to emphasise the “similarity and difference” comparison between countries' practices: if a practice in a certain country leans more on NPM-centric methods than the same practice does in another country, then that is going to be most likely visible in the former country's AI strategy.

Although NPM and GDPR are not necessarily each other's opposites, the two are very different and as such will intuitively have different effects on the AI strategies.

3.2. Validity and reliability:

There is always a certain uncertainty surrounding the usage of critical discourse analysis as well as an inductive strategy. For instance, is a qualitative focus on communicative events and, to a lesser extent, power the most suitable approach? Or could a more quantitative focus yield more conclusive
results? Could other terms by Fairclough been more well suited instead? How suitable are NPM and GDPR as secondary factors?

A qualitative method might be the most reasonable method here because of the focus on studying the text. A quantitative approach may have gotten a more comprehensive overview, but it may miss significant details. In addition, the aforementioned lack of articles delving into this topic justifies an inductive strategy: a deductive approach would need more articles that specifically discuss how privacy regulations affect AI strategies, and this is relatively unexplored territory. As for which terms are used, "Communicative events" are central to Fairclough's methodology, and "power" is closely related to communicative events, so the word choices are justified on those grounds.

The methodological approach is also open to criticism. This study is fully possible, even if not as overarching as a quantitative study would have been. However, placing the analysis in boxes might wind up contributing to the risk of missing significant details inadvertently. For that reason the analysis will be described in words.

It is also important to note that there may be few – or many - mentions of the word "privacy" in the AI strategies themselves. This is a risk that the study will have to acknowledge. That said, any mention of "privacy" will be treated as an indirect confirmation of privacy regulations' effects, so this study is not relying on there being a large sample size.

NPM and GDPR – while very different from each other – nevertheless exert significant influence on the three countries. These two secondary factors are also unavoidable to some extent – even if the reason it is unavoidable is partly due to the selection of countries. For that reason these two are included as important secondary factors and examples of where the AI strategies can diverge.

4. Previous research:

Papers that discuss specific nations' approaches to AI and related fields such as video surveillance and communication technology have been written over the course of the preceding decades. An example of these is "A Comparative Cyberconflict Analysis of Digital Activism Across Post-Soviet Countries" by Karatzogianni, Miazhevich and Denisova – which focuses on Estonia's handling of digital activism and privacy regulations in comparison to its more authoritarian post-Soviet neighbors as a contrast. Karatzogianni et al's paper is worth emphasising since their paper explores the different pathway Estonia took compared to some of its neighbors:

Björklund argues that "all discourses about surveillance contain a conflict between two values, expressed by each country's respective terms for privacy and security (often also defined differently in each context)." (Björklund 2013 p. 39) This is most starkly made clear in Karatzogianni et al's paper, where the impetus for Estonia to take a more liberal stance:

"The stark contrast of the Crimea and Belarusian digital activism to Estonia lies in the fact that the Estonian government is riding the wave of demands for digital rights, and transparency, as they have become the country’s public, social and digital policy agenda “ (Karatzogianni et al p. 13)

Papers that discuss privacy specifically in the context of internet usage have also been published. One example of this is Custers' et al's “Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies” - which defines informed consent as:

"In general, the process of providing consent is only considered fair when the person involved is
properly informed of what exactly he or she is consenting to and, to some extent, is (made) aware of
the consequences such consent may have. “ (Custers et al 2017 p. 3)

Custer's point has interesting implications for the study. It is the instances when consent is not given
that constitute a breach of privacy. One way that these breaches occur is when people are not
informed of the choice to begin with, and that emphasises the need for privacy regulations as well
as for the AI strategies to take those into account.

Out of the papers that specifically discuss how AI intersect with politics in general, two are worth
mentioning. Kulanovic's “The public leadership of artificial intelligence - How can challenges with
AI be handled?” directly discusses the case of how AI is affecting Swedish politics – particularly
Swedish leadership. In particular, the author tackles privacy – under the Swedish term “integritet”:

“The debate surrounding AI have become more positive under the latest years, but there still exist
increasing uncertainties such as not having control over AI, ethical uncertainties as well as the
negative effect on the work force. Acceptance and trust in AI within society is dependent on the
solution for other problems such as AI security, integrity and discrimination.” (Kulanovic 2019 p.
27).

Kulanovic enchoes this study's primary research problem: if potential problems such as integrity go
unnoticed or without solutions, then those uncertainties will increase. As was the case with the
Martinsburg Monster. And this is worth emphasising since those uncertainties will have significant
implications both for privacy regulations and AI strategies. The author also mentions the Swedish
AI strategy document, which makes it one of the few papers to mention a strategy document. (ibid
p. 37)

One caveat worth mentioning here is that there are not many other papers which look at the specific
topic of how AI strategies are affected by privacy legislation – which means that this is relatively
underexplored ground.

Still, one paper – Drake et al's “Legal contestation of artificial intelligence-related decision-making
in the United Kingdom: reflections for policy” delves into the British AI strategy and an ensuing
workshop intended to help address legal issues . The paper points out that the strategy has a tall task
ahead of it:

“But this new strategy must also address a big problem. Although it considers that its objectives‘
will be best achieved through broad public trust and support’, levels of public trust are low. A
deterioration in trust in the technology sector (or ‘techlash’) has been remarked upon globally (West
2021). It is certainly apparent in the UK, where already-poor perceptions of AI seem to be
deteriorating sharply. According to one survey, only about 32% of people in the UK trust the AI
sector of the technology industry. This is a lower proportion and falling faster than in any other
‘important market’ in the world with a drop of 16% since 2019 (Edelman 2020,2021).” (Drake et al.
2022 p. 252)

Drake et al's study emphasises the point that Kulanovic made – when people distrust the associated
technology or don't know the solution then faith in both privacy regulations and AI strategy
documents are undermined. This makes it more important to compare how the AI strategies are
influenced.

However, Drake et al's study also contradicts Kulanovic in tone – specifically when it comes to
framing the AI debate and trust. This could be explained by the two papers discussing some different aspects of the AI debate, as Kulanovic is discussing the possibilities and dangers associated with AI in society while Drake et al are bringing up how little people trust tech corporations specifically.

5. Material:

The material used will be sub-divided into a couple main categories: First, the chosen countries' strategies, accompanied by background detailing their history with AI and privacy. Additional material - primarily laws and additional articles - will also be included and used accordingly in each country's subchapter. Laws, torts and other official documents will be used as material to help explain how privacy is shaped, and news articles will likewise be used to

The material will be studied using the concepts outlined in the Theory and Methodology subchapters – using Björklund's three practices and Fairclough's concepts of communicative events and restraints as frames of references. This is because the material directly ties into the aformentioned research questions, and the material is intentionally chosen to help answer the research questions.

The selection of material was primarily done by first looking for the AI strategy documents – one for each country – and then by combing through official documents and news articles to select instances that specifically highlight interactions between the practices, as well as how the practices respond to additional factors such as NPM and the EU's GDPR.

The AI strategies were selected because they are central to their respective countries' goals and priorities. They may not necessarily intersect with privacy in all its sections, but the countries' AI strategies will have to take privacy issues into account by virtue of the technology. In addition, the AI strategies indirectly showcase how they are prepared, which may reveal which practice that are primarily shaping the strategies.

The AI strategies are selected with the caveat that since they might not primarily concern themselves with privacy. Still, this caveat should not detract from the main reason that these strategies were chosen.

The selection of material was also deliberatly chosen to emphasize instances where two or more practices interact; mainly to emphasize instances where the practices shape privacy-related legislation and torts. This is particularly the case with the news articles chosen: two of which involve different practices coming into conflict with the AI corporation Clearview and their surveillance technology, while the third one involve a confrontation between the Estonian government and a section of the Estonian public which spilled over to the Internet.

Newspapers articles related to AI and privacy will also be used to provide additional context – specifically to showcase significant events related to privacy. These articles might be where the public practice is most visible – since the practice is typically not directly seen in the creations of laws and torts. And while both the political-parliamentary and juridical-bueracratic practices can also be highlighted in articles those two practices are less dependent on the articles – they can communicate through their own official statements as well.

The main caveat with including newspaper articles is that these can skew how the public practice is
percieved. While this concern is not necessarily exclusive to newspaper articles – official
government documents have potentially similar issues – newspaper articles can paint one of the
practices or the other as overreaching. For the purpose of this study the newspaper articles will be
treated on a case-by-case basis in an attempt to allieviate this issue.

5.1. The case countries' history with AI and privacy:

Three countries have been selectively and intentionally chosen for the study. The choice of
countries intentionally avoids authoritarian states such as China: while authoritarian states have also
begun to use AI extensively, there is an argument to be made that authoritarian states will view
security as the state's security at the expense of citizens' – and privacy as something the state can
revoke immediately.

The United Kingdom of Great Britain and Northern Ireland, or Britain for short, is chosen since it is
arguably the birthplace of artificial intelligence as a research field; early pioneering efforts within
the field include Turing's seminal paper and Christopher Strachey's work during the 1950s
influencing subsequent developments.

The first British computers – the Manchester Baby and its successors, including the Manchester
Mark 1 and EDSAC – were built at universities. While the British government did sponsor this –
particularly through the predecessor encryption programmes and funding the university projects,
they remained heavily of scientific interest. This began to change as the British government took an
interest in computers to help simplify work of increasing complexity. (Agar 2006 p. 888)

While Britain had also joined the then EEC – later reformed into the EU in the 1970s; Brexit –
UK's process of leaving the European Union, which began in 2016 - further complicated matters.
By that point surveillance capitalism had been wellestablished. (Zuboff 2019 p.16) The fact that
they have followed EU's policies until relatively recently is worth noting in this context.

Resolving these differences is not going to be a simple matter: Britain has a long history with
privacy, directly based on one that Warren and Brandeis established. The British definition of
privacy is not enshrined in a specific Bill of Rights – instead it is based upon a legal tradition that
upheld privacy as a concept. (Wainwright v. Home Office 2003 § 15)

The word “privacy” “is derived from the Latin word "privatus" which means set apart from what is
public, personal and belonging to oneself.” (Online Etymology Dictionary 2020)

Sweden is chosen due to its early computing / AI response differed from the British. This is evident
in how the early Swedish computing industry developed: the earliest Swedish computers such as
BARK and BESK were developed after the Swedish Board for Computing Machinery
(Mattematiknämnden) and the Swedish engineering agency (IVA) took direct interest in American
hardware and explicitly meant to put those to their own use. (Hallberg 2007 p., 127)

Sweden does not have a word for privacy, which is notable in this context. "Integritet" is the closest
analogue here; albeit it is much more connected to the English word ”integrity”. The English word,
meaning "soundness, wholeness, completeness," comes from the Latin word from Integer. (Online
Etymology Dictionary 2020)

The concept of privacy – or integrity in the Swedish conception – did not emerge under the same
circumstances as the British concept did. Rather it came about during a time when the social
democratic government of Tage Erlander still held the political power, and old managerial paradigms within the bureaucracy still held sway. (Riksdagen 2004:51)

Estonia has what might be the most comprehensive governance system involving AI in place, and it serves as the most striking example where a democratic country has implemented AI.

Prior to 1991 it was part of the Soviet Union and as such partook in the Soviet computer (and AI) programme by virtue. The Soviet computer programme had lagged behind the West since the 1970s, and during the 1980s the shift to personal computers had yet to get a firm foothold the way it had in the UK and Sweden. (Stapleton & Goodman 1988 p. 6). While Estonia had an existing active computer base it also needed to develop said industry according to the Soviet 5 year plan, and both computer quality and production slipped severely as a result.

The Estonian word "Privaatsus" is likely a loanword from English, which probably shows some signs of English influence in this sector. (Online Etymology Dictionary 2000).

As a comparison, the Russian language has a couple words that could conceivably be translated as privacy: the first,"Конфиденциальность" - rendered Konfidentsial'nost' in the Latin script, does not share the same root nor same exact meaning: it would more appropriately be rendered "confidential", itself also sharing a Latin origin but with slightly different meaning. The second, "уединение" (rendered uyedineniye) is very likely from a Slavic language root, but it portrays solitude and seclusion.

A lot of Soviet computer and AI development happened to be located in Estonia, with the Institute of Cybernetics founded in Tallinn in 1960. (Tyugu 2007 p. 31) Estonia was one of the breakaway republics when the USSR collapsed, and its pre-existing computer industry was kept during the breakaway period. The country had already by 1988 inched closer to the West by signing a cooperation agreement with neutral if more west-leaning Finland. (ibid p. 32) And from the USSR's breakup Estonia started to lean more towards the West, including adopting Western standards on privacy.

5. 2. The countries' strategies:

The countries' strategies and how they have integrated AI into their respective governance methods will be used as primary sources.

These texts are particularly well-suited to answering the questions because they are not only government-produced and thus offer insight into the governments' own strategy making and communication; but also since the strategies potentially showcase differences in intent between the respective countries' political practices.

The strategy texts are also important because they showcase how the political-parliamentary practice interacts with the juridical-bureaucratic practice in each country: a very important consideration since the two are implicitly intertwined.

One counterpoint here is that the strategies might not meaningfully include everything that goes on between the political-parliamentary and juridical-bureaucratic practice; nor might it even include the public practice' means of communicating or interacting with the other practices: as such it necessitates the usage of other material is justified on those grounds. Still, the strategies remain the primary material used because of their importance to answering the questions.
The UK enacted its own strategy presented in Parliament during September 2021. The strategy emphasises the perceived need for the UK to become an AI superpower, with the division of three different categories being perceived as instrumental to these goals.

Sweden's position on integrity is affected by the GDPR since it – unlike the UK - is still an EU country. As such it means that Sweden's position is affected by the country remaining within the framework. It is important however to note that this is by no means all-encompassing; a framework is not typically meant to give political-parliamentary and juridical-bureaucratic solutions for every single issue within a country.

The government's “Nationell inriktning för artificiell intelligens” - produced by Näringsdepartementet or the Ministry of Enterprise and Innovation - outlines the general strategy towards AI: it is mainly predicated on international competition, with the opening paragraphs highlighting this. Not only is there a strong link established between AI and digitalization, but the paragraphs also highlight that AI have the potential to aid economic growth and public welfare.

When Estonia became independent its proximity to the much larger Russia indirectly lead to the country joining the EU in 2004, the country began to look towards the West for its geo-political security and started to approach it culturally too. This is visible not just by adopting the words “privaatsus”, likely an English loanword, but also because it integrated itself much more closely to the Western scientific world; indigenous computer scientists like Tyugu traveled mostly to Western countries post-independence.

Estonia's AI strategy – “Estonia’s national artificial intelligence strategy 2019-2021” produced by the Ministry of Economic Affairs and Communications (MKM) – mainly focuses on AI as a method to inform public and private activity. In particular it incorporates a comprehensive schematic for governmental agencies: this differs from Sweden's and the UK's respective strategies in that specific governmental agencies are tasked with enacting specific projects. In effect suggesting that Estonia's government has already developed significant tools for governance.

The Estonian AI strategy's action plan is detailed to the point where its suggestions wound up leaving a visible trail in subsequent strategy texts: MKM's “Estonia’s Digital Agenda 2030” directly references the Estonian AI strategy and will be used to complement the AI strategy.

**5.3. Laws, torts and other governmental documents:**

Laws, torts and governmental documents are a significant portion of the material, and chosen because they define privacy legislation in each country studied. The laws, torts and governmental documents are intentionally picked when available – which inevitably means that they will be dependent on the countries in question.

The documents are also chosen because they add additional context to the strategies and help to illustrate why the strategies prioritize certain aspects of AI policy. While the documents are not necessarily directly connected to the strategy documents the influence that official documents have on the strategies is still notable.

A significant caveat with these documents is that they – like the strategies – may not sufficiently cover what the public practice does in order to affect privacy regulations. This caveat is not entirely detrimental to the documents' relevance, but it is nevertheless a significant issue that needs to be
Several documents are of particular interest here:

Wainwright v. Home Office is a British court case which established a key privacy precedent in 2003. This court case arose from a dispute between two private persons – Mr. Alan Wainwright and his mother – on one side, and the Home Office on the other. The Wainwrights had been reluctantly stripsearched for drugs during a prison visit, and Alan in particular had suffered enough emotional distress to cause PTSD. As such, the presiding Judge concluded that the stripsearch was necessary nor proportionate (Wainwright v Home Office 2003). The court case is worth noting since it is a case where the juridical-bureaucratic practice directly set a precedent – implying that the practice is actively using its means of communication to establish new privacy-related laws.

The Swedish Riksdag passed one of its first privacy-related directives in 2004, named “2004:51: Skyddet för den personliga integriteten“. The directive noted that while privacy have been discussed to some extent for the preceding forty years, the need for new directives and laws had become apparent for crime fighting reasons. (Riksdagen 2004:51) While it is contemporary with Wainwright v. Home Office, it did not originate from the juridical-bureaucratic practice – instead it was the political-parliamentary practice publishing the directive and re-initiating the discussion on its own terms.

Estonia's government published a Digital Agenda document called “Digital Agenda 2030 (MKM 2021) This document was published shortly after Estonia's AI strategy, and showcases an more overarching overview of what the Estonian political-parliamentary practice wants to achieve. This particular Agenda document is notable since it was published very soon after the Estonian AI strategy by the same ministry behind the strategy as well.

Those three are not necessarily alone, but they take on significance because of their background importance to the strategies. While neither Wainwright v Home Office nor “Skyddet för den personliga integriteten” primarily involve AI, those two are nevertheless chosen because they have significant implications for when AI is used. One example of this is video surveillance, which uses AI to track individuals' movements.

5. 4. News articles:

News articles are another significant portion of the material – not only since they provide additional context to both the strategies and the official documents, but also since the artincles do not originate from the political-parliamentary or juridical-bureaucractic practices.

Their inclusion into the study is mainly done to alliviate the previously discussed problem of strategies and documents not covering the perspectives coming from the public practice. Since news articles are typically written within the public practice they are also coming from a perspective that may not be entirely visible if this study were to solely focus on the strategies and other official documents.

The central caveat with the articles is that the ones chosen are going to react to events occuring: while news articles are not necessarily reactive most articles are, and finding news articles that predict shifts in privacy policies seems intuitively like a very difficult exercise. The caveat means that news articles are going to be used not when practices are anticipating an occurrence; rather when they are reacting to those occurences.
An important example of news articles are ones that deal with the video surveillance corporation Clearview. These are included not only to emphasize the role that NPM can play in affecting countries' and practices' discourse usage, but also to provide cases where there are pushback against corporations. Those cases of pushback, in turn, give examples of where NPM-centric solutions also reach their limit.

6. Analysis:

6.1. United Kingdom:

The British definition of privacy was established relatively early on. It originate from court cases where a complaint was levied – one example being Wainwright v. Home Office – and as such typically respond to the specifics of the case. Wainwright v. Home Office's 15th paragraph highlight this by drawing on Warren and Brandeis' article:

“My Lords, let us first consider the proposed tort of invasion of privacy. Since the famous article by Warren and Brandeis (The Right to Privacy (1890) 4 Harvard LR 193) the question of whether such a tort exists, or should exist, has been much debated in common law jurisdictions. Warren and Brandeis suggested that one could generalise certain cases on defamation, breach of copyright in unpublished letters, trade secrets and breach of confidence as all based upon the protection of a common value which they called privacy or, following Judge Cooley (Cooley on Torts, 2nd ed (1888), p 29) "the right to be let alone". They said that identifying this common element should enable the courts to declare the existence of a general principle which protected a person's appearance, sayings, acts and personal relations from being exposed in public. .” (Wainwright v Home Office 2003 § 15)

The notion of ”privacy” is thus in the British tort system heavily contingent on juridical precedents. The torts effectively helps the British juridical-bureaucratic practice create a content constraint, where the juridical-bureaucratic practice is effectively using the language itself to constrain further political action and communicating that way.

This has an interesting effect on the British AI strategy: it uses ”privacy” three times, and the strategy is keen on communicating that it will not undermine privacy:

“The Office for National Statistics (ONS) is leading the Integrated Data Programme in collaboration with partners across government, providing real-time evidence, underpinning policy decisions and delivering better outcomes for citizens while maintaining privacy. The 2021 Declaration on Government Reform sets out a focus on strengthening data skills across government including senior leaders.” (UK Government 2021 p. 18)

Notably, the government is trying to signal that they are maintaining privacy - which in turn is indicative of the political-parliamentary practice not wanting to undermine precedents. The AI strategy – produced by the government – is leaning on wording that the juridical-bureaucratic practice provided, and as such is not seeking to undermine the constraint that the juridical-bureaucratic practice established.

The British strategy divides its goals into a cross-table, three sections: short, medium and long term, suggesting that the framework for developing AI policies is thoroughly established by the government. (UK Government 2021 p. 2)
First, "Investing in the Long Term Needs of the AI Ecosystem" - which is mainly predicated on infrastructural needs, but also includes a passage about protecting internal security while also keeping the UK open to business. This does propose wide sweeping changes and integration of AI into UK's socio-political sphere, even if it risks running into the problem of security clashing with privacy. The second, "Ensuring AI Benefits All Sectors and Regions " is more focused on expanding the diffusion and adoption of AI, while the third, "Governing AI Effectively” is more directly concerned with ethics, which is evident in the medium term goal “Establish medium and long term horizon scanning functions to increase government’s awareness of AI safety ”. (UK Government 2021 p. 6)

There is also one long term goals worth emphasising: ”Work with partners in multilateral and multi-stakeholder fora, and invest in GPAI to shape and support AI governance in line with UK values and priorities . It not only puts a spotlight on the international cooperation that the UK values strongly, but also indicates that the British strategy embraces NPM to some degree.

It is especially important to note in the case of multilateral and multi-stakeholder fora, where inevitably some form of competition will emerge. While data will – in this case – inevitably be shared between the organisations involved it also creates a certain risk that the organisations will clash over which data to share and which to not share. It also depends heavily on which type of data is shared in these situations.

Either way, one inference one can make here is that professional management becomes very important for organizing and executing the various projects, but these can create situations where it becomes difficult to track different projects – specifically if the projects are divided between experts and corporate entities.

This is not a simple process – one can make the argument that surveillance capitalists want to avoid every single constraint. (Zuboff 2019 p. 309) This creates a major problem for an NPM-centric governance structure: if a governance structure wants to emulate corporations and corporations themselves want to eliminate as many constraints as possible, then it risks severely undermining the constraints that the governance structure wants to maintain.

Here it is worth noting that the goal itself is rather vague – multilateral and multi-stakeholder for a can take on multiple different meanings. Although in this case, it might be worth looking at what “UK values and priorities” entail. As such, it might be worth diving into news articles in order to clear that up.

In November 2021, The UK Information Commissioner Office (ICO) ordered Clearview AI – a facial recognition company - to stop processing all user data “for failing to inform British residents that it was collecting billions of photos from sites including Facebook, Instagram and LinkedIn to build its facial recognition software.” (New York Times 2021)

The ICO is an independent body which reports directly to the British parliament, making it a case where one could argue it is part of the political-parliamentary practice. The Information Commissioner stated:

“I have significant concerns that personal data was processed in a way that nobody in the U.K. will have expected,” (ibid)
This sentence emphasises that the ICO's “significant concerns” arose from Clearview not informing the British public, and thus becomes a form of creating reality through the language. Clearview's actions are dangerous and something to be feared because the British public's not informed, just as the Martinsburg Monster was built without informing the American public.

The Clearview fine has significant implications for the AI strategy itself – particularly in the context where the British government wants organizations to engage in AI uptake, but are concerned that privacy regulations are hindering said uptake. Which in turn could imply a very difficult choice for the British political-parliamentary practice: either cooperate with surveillance capitalists who might undermine the constraint system and public trust further when it has already dropped in Britain; or restrain the surveillance capitalists and risk slowing down the AI uptake. (Drake et al 2022 p. 252)

The ICO stated in their press release on the fine that “The joint investigation was conducted in accordance with the Australian Privacy Act and the UK Data Protection Act 2018. “ (Information Communication Office May 23rd 2022). The Data Protection Act 2018 is one of the laws that the ICO covers, and as such the ICO gained its enforcement abilities from the DPA. (ibid 2023).

This act was meant to replace both the previous Data Protection Act 1998 and EU's General Data Protection Regulation; but the GDPR's influence is evident in how the DPA defines ”public authority” and ”public body”:

"For the purposes of the GDPR, the following (and only the following) are “public authorities” and “public bodies” under the law of the United Kingdom—
(a) a public authority as defined by the Freedom of Information Act 2000,
(b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13), and
(c) an authority or body specified or described by the Secretary of State in regulations,” (Data Protection Act 2018 §7.1)

The main implication that the DPA – and the FoIA by proxy - have for the AI strategy, however, is relatively counterintuitive. The strategy itself notes:

“The UK data protection framework (UK General Data Protection Regulations and Data Protection Act 2018) is technology neutral and was not intended to comprehensively govern AI systems, or any other specific technologies. Many AI systems do not use personal data at all. “ (UK Government 2021 p. 28)

The strategy is thus noting that the law – although intended to strengthen privacy regulations – is not intentionally steering the regulation of AI policies. As a result, the strategy itself is left in a state of relative flux:

“Navigating and applying relevant data protection provisions can be perceived as a complex or confusing exercise for an organisation looking to develop or deploy AI systems, possibly impeding uptake of AI technologies.” (ibid)

When the strategy itself wants to encourage an uptake of AI technologies, it is also acknowledging that doing so is a potentially bewildering task for these organizations. The strategy itself thus is noting that the political-parliamentary practice is not the primary communicator: if it were then the DPA would have instead been intended to govern AI system.
The DPA still has an unintentional effect on the strategy – it is potentially contributing to the confusion – but it is not having an intentional effect. But the data protection provisions still retain relevancy because the strategy acknowledges they are important to navigate.

The DPA's process shared similar beginnings as the GDPR, but diverged on account of its introduction and its political-parliamentary process. The DPA was introduced by the parliamentary under-secretary on 13 September 2017, and both the royal assent and the subsequent amendment came around during a time when Britain was in the process of withdrawing from the EU – which culminated in the European Union (Withdrawal) Act 2018.

When Lord Frost, then-Minister of State at the Cabinet Office, gave an oral statement to Parliament September 16th 2021, he framed the withdrawal process and data rights regime creation as an opportunity:

"We intend to create a pro-growth, trusted data rights regime, more proportionate and less burdensome than the EU’s GDPR.” (House of Lords September 16th 2021)

This kind of language is often replicated in the UK strategy itself, which not only mentions “growth” twenty-eight times, but also makes “growth” a central theme – effectively seeking to create a reality which growth, trust and privacy can co-habit. For instance, one of the assumptions the strategy makes for the upcoming ten years is that:

“Our governance and regulatory regimes will need to keep pace with the fast-changing demands of AI, maximising growth and competition, driving UK excellence in innovation, and protecting the safety, security, choices and rights of our citizens. “ (UK Government 2021 p. 5)

The national strategy not only follows Lord Frost's comments, but the national strategy also follows the Minister's desire to adopt a corporate-friendly solution if possible. It does not mean that it is entirely friendly to corporations – like the case with Clearview showed – but it is nevertheless aiming to follow and even maximize an NPM-centric solution. As such, the political-parliamentary practice – represented here by Lord Frost – is creating a reality where Britain might need to follow such a solution.

The number of times “growth” has been used compared to “privacy” would suggest that the political-parliamentary practice is much more interested in growth: however, it is also worth mentioning that “growth” is never meant to directly contradict “privacy” - which could suggest that “privacy” takes a primary role here despite being used less.

However, Drake et al issued a warning in their paper – particularly noting that the promises of reforms are vague:

“In the context of low trust and growing contestation, ideas for new arrangements will seem vague and unreliable compared to specific plans to remove perceived legal obstacles to the present direction of AI-related decision-making (e.g.much more detailed proposals Q4.4.4-7 on ‘public interest’ processing, 4.4.8 ‘streamlining’ matters for the police on biometrics, 4.5.1 on ‘public safety’ justifications).”(Drake et al 2022 p. 275)

The ensuing direct accusation that the government is not creating a trusted data rights regime – rather dismantling it – is a major charge to make, but one that is rooted in a direct distrust that Lord Frost and other members of the political-parliamentary are actually following through with their
“For example, it is proposed not just to abolish DPIAs (Q2.2.7-8) but to remove Art.30 GDPR record-keeping requirements (Q2.2.11). Such measures appear likely to ‘hinder effective enforcement’, despite the claim that the risks will be ‘minimal’” (ibid)

The British practices are thus in an uneasy position, but the practices are still active:

As for how Britain's privacy regulations are shaped - it is evident that the British privacy regimen is chiefly one where the torts set the precedents and the juridical-bureaucratic practice is the main force driving these. Wainwright v. Home Office is one key example, and one that set precedent for the British government's regulation of AI. The political-parliamentary practice is largely following, although its use of communicative events suggest the faction is not entirely comfortable.

The statements as well as the national strategy can also reveal some cues as to which direction privacy regulations are currently heading. The national strategy leans heavily on dialogue between the government and outside organizations. In particular, comments like Lord Frost's emphasise a willingness to use the British regimen to diverge from the EU's norms and embrace a NPM-centric solution.

Lord Frost's “pro-growth” comments could unintentionally create a number of issues for Britain: such as outsourcing possibly leading to surveillance capitalism. In turn, that surveillance overreach could necessitate the juridical-bureaucratic practice's intervention as with Wainwright v. Home Office. It is not an unreasonable position when Drake et al argue that the political-parliamentary practice's actions could lead to the dismantlement of the data rights regime – it also might undermine the ICO's position as enforcer.

The second question – how the practices interact – is thus relatively straightforward. The juridical-bureaucratic practice has a lot of independence when defining privacy legislation and indirectly affecting the AI strategies – as evidenced by the torts. The British strategy does mostly heed to its language, and thus the juridical-bureaucratic practice play the primary role. The political-parliamentary practice is also very active due to them adopting and changing laws as well as shaping regulations, although they play a secondary role to the juridical-bureaucratic practice.

The two are relatively independent from each other, and exercise authority from a position of strength – however, the political-parliamentary practice's position in the constraint system is not entirely clear due to its NPM structure and interactions with non-governmental actors. The juridical-bureaucratic practice's influence looks to be much more apparent however, even if “privacy” is used less by the national strategy than “growth”. In particular, the juridical-bureaucratic practice is primarily focused on using the content constraint to indirectly steer the national strategy's word choices.

There are a couple caveats worth noting here though. In particular, the public practice is not particularly active when it comes to formulating AI strategies or the privacy discussions; the public is arguably visible in Wainwright v Home Office due to a private person starting the legal process, but even then that does not take place in a public arena of debate. Otherwise, the public practice does not affect privacy regulation nor AI regulations as much.

The interactions between practices are primarily through legal documents and governmental records. The governmental records hint that the political-parliamentary practice's activities is the
most widespread since it leans into NPM. Not just with Lord Frost's comments, but also due to them consulting corporations. How much the British government leans into NPM is somewhat difficult to tell, partly because the strategy's comments about multi-stakeholder for a is relatively unclear, but also since the Clearview case shows that the extent has a limit.

The government's actions have been heavily criticized by Drake et al. - and that criticism may presage a significant turn in social relations between the political-parliamentary practice and the other practices should the political-parliamentary practice indeed continue to dismantle the data rights regime.

6. 2. Sweden:

The Swedish approach has a lot of similarities with the British – which is visible when the strategy bases itself heavily around the notion of being a world leader in AI – and the strategy puts some major emphasis on the notion that AI should be viewed as a priority:

“An active support for AI applications in the public sector might have major importance for how the public sector manage to meet the great societal challenges of the future. Official actors should therefore actively support AI applications through, with regard given to security and integrity, make available the relevant data and develop a national infrastructure.” (Näringsdepartementet 2018 p. 5)

The strategy as such relies heavily on research, development and innovation as a central tenet. While the British strategy likewise highlighted research as one of the central areas the Swedish strategy instead aims to “develop a national infrastructure” - which in turn implies that one is not already in place. This is already a stark contrast to the British strategy, which implied that it had a programme in place already.

Another significant contrast to the British strategy is the lack of a tabled roadmap: instead, the Swedish strategy has chapters dedicated to specific conditions: “Education”, “Research”, “Innovation and use” as well as “Framework and Infrastructure” as the principal subdivision. (ibid) This subdivision focusing on education, research and innovation figuring into a framework indicates that the Swedish strategy is to be developed and applied on a wide scale.

The usage of “integritet” is also noticeable here. Like the British strategy the Swedish counterpart is focusing on “integritet” as a factor to not be undermined: “integritet” is mentioned three times throughout the text compared to “growth” being mentioned twice.

However, the Swedish strategy focuses much more on relevant data when developing a national infrastructure, whereas the British strategy takes it as a given that the data will be relevant. This leads to an interesting inference: the Swedish strategy is taking a more cautious approach to AI, although it might be because the national infrastructure is not fully developed.

The Swedish strategy also points out that: "Sweden is a [relatively] small country with a small internal market” which in itself means that developing partnership with actors from other countries becomes essential. In particular the Swedish strategy mentions the EU as an important arena to develop the partnerships in -, and directly names GDPR as an example to follow. It is a significant divergence from the British strategy, which aims to move away from the EU. (ibid p. 9 - 10)

While both the Swedish and British strategies emphasize NPM-centric solutions – particularly with how the Swedish strategy uses the term market - the Swedish strategy words it in a way that not
only highlights international cooperation but also creates a need to coordinate these under one banner. In particular, phrases such as “continuously see over the need for a digital infrastructure to capture the opportunities that AI can give” indicate that the Swedish strategy seeks to communicate the need to create a framework. (Kulanovic 2019 p. 41)

The strategy also puts a lot of emphasis on a framework-centric solution, which is effectively adopting the GDPR's system. However, there is a major caveat here, in that the GDPR's and the strategy's respective frameworks are not necessarily the same. In a way the strategy highlights this by taking a more reactionary approach – which is not necessarily compatible with the GDPR's framework-centric methods.

It still begs the question of what causes this divergence in the respective national strategies' contents. There is an implication that the Näringsdepartementet are directly looking at the issues that the Swedish system has encountered – but an admission that a national infrastructure does not entirely exist yet does not fully confirm any of the practices' influence by itself, even if the inference can be made.

The legal pretext for AI has also developed somewhat differently in Sweden. In particular, it did not develop in a pre-existing tort-centric environment, instead the legal pretext developed more recently. One such case is the Committee Directive 2004:51, which specifically deals with protection of personal integrity: (Riksdagen 2004:51)

“In Swedish lawmaking there is no definition of the term personal integrity. In different inquiries (see for example “Tvångsmedelskommitténs betänkande Tvångsmedel - Anonymitet - Integritet [SOU 1984:54 s. 42”]) one has by using amongst others the basic freedoms and rights outlined in The Instrument of Governments second chaper as a starting point tried to mark a precise definition by separating spatial integrity (integrity at home), material integrity (property rights), bodily integrity (protection for health and wellbeing, against invasion either in or against the body), personal integrity in a physical sense (protection for personal freedoms and freedom of movement) and personal integrity in an ideal sense (protection for private life and for the individual's personality including the private economy.)”

If anything, the Committee Directive has an already significant indirect influence on the Swedish AI strategy because it invokes the Instrument of Government as a definitional starting point for integrity and thus setting up a content constraint for any subsequent regulations.

As such, this constraint being tied to the Instrument makes it apparent that the Swedish political-parliamentary practice has a primary role in shaping these regulations. Despite there being no definition of the term when the Directive was written, it is clear that the Swedish political-parliamentary practice has been attempting to frame privacy discussions under specific terms. In this case, data and AI falls under the “personal integrity in an ideal sense”, data shouldn't be made available without the regard to security and integrity.

This is echoed in the AI strategy document, where it notes: “Ethical and security-related considerations should not be an afterthought in AI applications, but must be an integrated part from an early stage”. (Näringsdepartementet 2018 p. 5)

However, the implication that discussions have taken place since the 1960s also implies that there have been little movement in that forty year span. This is an interesting contrast to Britain, where Wainwright v. Home Office drew upon the Information and Communication Act.
Still, the 2004 directive is also useful for looking at specific developments within privacy as a legal concept. The concept being relatively new compared to the British one does mean that it has not had much time to develop: instead, in the Swedish case the concept of integrity has been adopted by the political-parliamentary structure. In many ways, this fitting-in happened relatively recently and was an attempt by the Swedish government to augment the existing system.

This is evident in SFS 2007:975, the regulation that established the IMY (Integritetsskyddsmyndigheten, or The Ministry of Integrity Protection). The first paragraph is clear in laying out IMY’s mission:

”The Ministry of Integrity Protection's chief task is to ensure that peoples' basic freedoms and rights are protected when it comes to social security numbers, to ease the free flow of such information in the European Union and ensure that good practice is followed when it comes to credit information and debt collection work.” (SFS 2007:975)

SFS 2007:975 also authorised the IMY to handle video surveillance in the second paragraph, citing the camera surveillance law (2018:1200). What's additionally worth noting is that the IMY is considered part of the Justice Department, and thus a piece of the juridical-bureaucratic process. (SFS 2007:975)

It's also worth noting that the juridical-bureaucratic structure is thus directly subordinated to the political-parliamentary process, both in terms of the content constraint and the subject constraint. However, the juridical-bureaucratic process also gains its constraint power from the political-parliamentary one: particularly in that SFS 2007:975 authorises the IMY to monitor social security numbers.

As such a relation is also formed – one that allows the Swedish political-parliamentary the ability to create new laws, while the juridical-bureaucratic practice is given the ability to enforce them.

In one particular enforcement case, the Swedish police got a major fine in 2021 from IMY because they had used Clearview's AI program without first announcing that they were doing so – the Police argued that only a few police members had used the AI, but it did not prevent the fine. (SVT 2021).

IMY's comments were primarily that the Police had not properly announced that they were going to use Clearview's AI, that they had not undertaken the appropriate organizational methods; as well as infringing on the local crime data law by using biometric information without first reviewing the use for consequences appropriately. (ibid)

In particular, IMY emphasised that the Police had “vulnerabilities in several areas” when it came to handling personal information – which indicates that the IMY is using that discourse as a way to reprimand the Police and use its own language and enforcement powers to restrain the Police.

In addition, this incident also showcases that outsourcing solutions to corporations can sometimes wind up backfiring: the police conducted this outsourcing of personal data without telling other governmental agencies or the public about it. In effect the police themselves wound up undermining the constraint system – particularly the relation constraint, since the police undermined it by using Clearview’s AI without informing others. The subsequent reprimand and fine could thus be seen as the IMY reminding the police that the relations constraint should not be weakened this way.
IMY's and the Police's different viewpoints also correlate strongly to Björklund's main point: that security and privacy do not always coincide, and indeed can oftentimes wind up diametrically opposed to each other. (Björklund 2013 p. 39)

It provides an interesting comparison and contrast to Britain's handling – although the UK Information Commissioner Office directly asked Clearview to halt its data collection whereas the IMY asked the Swedish Police instead.

This communicative event between the IMY and the Police is indirectly reflected in the AI strategy document: not just by the perceived need to rally the entirety of Swedish society under one framework, but also in that the AI strategy emphasises cybersecurity as an area where more competence is needed:

“Today there is a lack of people with AI competencies in Sweden as well as in foreign countries which leads to a tough competition surrounding personnel. As the use of AI increases the risk that lacking competence poses becomes more clear. In order for broader usage of AI to become possible it is required that Sweden educates enough people in the area.” (Näringsdepartementet 2018 p. 6)

The strategy is interestingly using similar language as the IMY, despite the strategy not mentioning the incident nor blaming either party. But the AI strategy is using this communication to help create the reality that more people need to be educated in AI usage.

The perceived lack of AI competence could help to explain the lack of movement in this area: particularly since the “Swedish arguments in favour of video surveillance have strongly emphasised its utility in preventing crime” dating back to the 2000s, when the Committee Directive was adopted. (Björklund 2013 p. 39) It is possible to infer that the police took a simplistic view of AI as a crimefighting tool, one that dates back to this period.

Judging by the fact that the news coverage at the time was not entirely pervasive – the Swedish public prosecutor did take the notion of “security = privacy” to its logical extreme in 2005, and yet a newspaper article a year later quoted three top dignitaries as essentially using the same logic without it resulting in a significant public reaction. (ibid p. 42)

How Sweden adapts GDPR is worth noting in this context, since the GDPR has spurred the Swedish political-parliamentary practice to publish the AI strategy document – where it calls for further education. The adoption of GDPR was enacted in the Riksdag law 2018:218 as well as the Justice Department's regulation 2018:219. The former directly complements EU’s 2016/679, and the terms used are made the same as the one in the EU's. The latter supplements the law by appointing the IMY as the primary overseeing authority:

“In Caritis byckdsmyndigheten is a supervisory authority according to EU’s data protection regulation and the law (2018:218) with complimentary decisions to EU's data protection regulation. Regulation (2020:1140)” (Swedish government 2018:219 3 §)

In comparison to the British DPA, the Swedish implementation of GDPR does differentiate itself – not only since the Swedish implementation does base its implementation directly on the EU's instead of shunning it, but also since the Swedish political-parliamentary process granted the IMY the enforcement power. While it was adopted from the EU, it was introduced through a political-parliamentary process in the Riksdag, and then applied into the juridical-bureaucratic one through the domestic regulation.
How IMY works in this context - as an enforcer within the juridical-bureaucratic practice – also emphasises that Sweden's bureaucracy retains some key enforcing power to shape discourse, like with the Police fine. It emphasises that political-parliamentary control over the juridical-bureaucratic process still exists to a large extent.

This political-parliamentary control of the juridical-bureaucratic process does not however exclude agencies within the juridical-bureaucratic practice from forming their own partnership: the police could form their own partnerships with partners outside of Sweden.

As for how Sweden regulates privacy, it differs some from the British interpretation. While privacy-related matters are handled as a juridical-bureaucratic matter underpinned by political-parliamentary processes, here the political-parliamentary practice took the first steps by recognizing something needed to be done.

Likewise, developments within privacy law are not established by the juridical-bureaucratic process; rather, they are first submitted and processed through the political-parliamentary practice, in this case through the Riksdag first requesting a review (such as the 2004 Committee Directive) and then establishing the necessary privacy regulations and institutions.

How the practices interact is relatively straightforward. The Swedish governance system leans heavily on the political-parliamentary practice to legislate new privacy-related laws while the juridical-bureaucratic practice is tasked with enforcing those laws – including restraining itself and the political-parliamentary practice as evidenced by the IMY having the ability to prosecute the Police and other governmental organizations. The constraint system used is primarily relational between the government and the IMY, although the contents themselves are frequently used to help enforce the relational constraint. This is a notable contrast with Britain, where the juridical-bureaucratic practice is the primary legislator and uses contents primarily to shape speech and thus legislation.

Whether or not Sweden is indeed using NPM as a basis for their AI work is rather difficult to answer. On one hand, the strategy is directly calling for multilateral actions and building connections with multinational actors. On the other hand the Swedish bureaucracy still inherits notions that specific agencies ought to watch over agencies as well as corporations; and take action if needed. Likewise, the AI strategy's emphasis on framework solutions does mean that the NPM solutions are not unrestrained.

The combination itself hints at a multilateral system; albeit one where the stakeholders are subject to review by an state agency - IMY. Corporations here act not just as partners to various agencies such as the police; but they also are outlined by the strategy as a neccessary part of the system; thusly implying that NPM does have some influence within the Swedish bureaucracy. Unlike Britain and the ICO, it does not appear as though the Swedish political-parliamentary practice is actively undermining the system.

One can certainly make the argument though that even as NPM underpins interactions between agencies and corporations the older social democratic model still survives to a certain extent. This is not only visible in IMY taking on a more overarching role as enforcing the law and regulation, but also since the IMY is integrated into the Justice ministry,

And as for where the interactions between the practices can be seen, those interactions are like
Britain typically seen in laws as well as bureaucratic documents. Most of the day-to-day actions are taken via the bureaucracy such as the Clearview and IMY cases, although the overarching framework is set up through the laws.

Like the British public practice the Swedish public is rather conspicuous in its absence. This may be partly due to selection bias – the cases that have involved IMY have generally been cases where the agency has fined another agency citing the law as well as the regulation.

This does not necessarily mean that the Swedish public is altogether absent from developing notions surrounding AI or privacy; after all it is reasonable to assume that the Swedish public would have some interest since ordinary citizens may not be passive.

The lack of Swedish discourse surrounding video surveillance may come down to the fact that it is mainly being framed as an issue of crime prevention within the political-parliamentary and juridical-bureaucratic practices and not expanded into a wider debate with the public practice. (Björklund p. 42)

This explanation is rather rickety however, since if the same assumption is extended to the public practice it can lead to the implication that the public is uninterested in privacy. Which would be an absurd inference and conclusion. The more likely explanation is to not go that far, but instead say that the lack of debate regarding video surveillance instead might be the result of privacy being mainly seen as a matter for the political-parliamentary and juridical-bureaucratic practices to handle.

Regardless, the lack of a public debate remains an interesting aspect of the Swedish discussions. This might be attributable to the lack of education that the AI strategy noted. The lack of education is still a potentially major issue here – with the incident between the IMY and the Police being a key case in point, but also an issue Björklund noted. (ibid 2013 p. 45).

However, the interplay between the political-parliamentary and juridical-bureaucratic arenas are by far the most visible, specifically with the Instrument itself being cited as a mean to try and establish a concept of privacy.

The usage of AI in the Swedish governance system is primarily defined from the perceived need to cooperate with non-governmental actors as well as surveillance in the name of crime fighting. However, the political-parliamentary practice's implementation uses elements of different managerial systems – such as an arguably deeper reliance on NPM compared to Britain – contrasts to a significant degree with the still-existing bureaucratic structure and how it has kept at least some elements from the traditional governance form.

6. 3. Estonia:

The Estonian approach to AI can be seen as its own case, primarily since the AI strategy is based upon an internal systematic solution rather than a strategy that leans much more towards becoming a "world leader" in AI:

“In May 2019, an expert group led by Ministry of Economic Affairs and Communications (MKM) and Government Office presented proposals on advancing the take-up of artificial intelligence (AI) in Estonia aka for Estonia’s national AI strategy (hereinafter: strategy).

This current strategy has been prepared based on these proposals, as a plan on how to implement the
expert group’s recommendations. It was adopted at Cabinet meeting on 25 July 2019. “ (KRATT - MKM 2021 p. 1)

From the immediate start it is evident that the Estonian government is taking a direct approach: the Estonian AI strategy is arguably more directly controlled by the Estonian political-parliamentary practice than its British and Swedish counterparts. It is particularly evident in how the experts themselves are tied to the MKM, but also in how it was adopted at a Cabinet meeting. - while the British and Swedish strategies are also tied to government organs the Cabinets are not as directly involved there.

As such the Estonian political-parliamentary practice is more directly noting down the contents of the AI strategy itself: the MKM and the expert group in general is also directly setting a relation constraint:

“The strategy is a sum of actions that Estonian government will take to advance the uptake of AI in both private and public sector, to increase the relevant skills and research and development (R&D) base as well as to develop the legal environment. This strategy is also Estonian national AI strategy in the European Union’s coordinated AI action plan context, synchronised with and supporting relevant EU-level activities. “ (ibid)

The strategy directly touches on “both private and public sector” which indicates some level of interaction with corporations and thus NPM, but the government is looking to do so on its own terms.

The Estonian AI strategy divides itself into four categories – not entirely unlike the British strategy – but they are not subdivided on a temporal scale. Rather, they are subdivided according to four categories: “Advancing the uptake of AI in public sectors in Estonia”, “Advancing the uptake of AI in private sectors in Estonia”, “Developing AI R&D and education in Estonia” as well as “Developing legal environment for uptake in AI”. However, the last category concludes that “There is no need for fundamental changes to the basics of the legal system, but there are some changes in different laws to be made. “ (ibid p. 10)

The division is interesting in itself since it is focused on building up the AI infrastructure. While both the British and the Swedish strategies also made a lot of effort to highlight AI uptake, what makes the Estonian strategy notable is that the Estonian political-parliamentary practice is directly using its own wording to set the aims.

The words “privacy” and “growth” are both conspicuously absent from the strategy, but point 1.6: “Develop principles for responsible use of data” had a both an objective: “Drafting a proposal for responsible use of data (principles)” as well as a deadline: “December 2019 submission to Cabinet meeting”.

The commitment to “responsible use of data” in turn lead to a follow-up strategy document produced by MKM called “Estonia’s Digital Agenda 2030”, where this lack of clarity regarding privacy was indirectly noted – and the “Digital Agenda” document directly cited the AI strategy document:

“Artificial intelligence has been adopted in the public sector on the basis of Estonia’s national artificial intelligence strategy and the first results have been achieved. As of the end of 2020, approximately 80 AI projects have been implemented or are ongoing. Nevertheless, competences
related to artificial intelligence and data science are lacking, the level of implementation of Estonian language technology is still low and there are legal obstacles to the use of data (for example in connection with interpreting data protection requirements). Algorithmic trustworthiness has not been systematically guaranteed in the implementation of AI yet. “ (MKM 2021 p. 16)

The Estonian strategy thus has an effect on subsequent official documents, something which is not as readily apparent in either the British or Swedish strategy documents. Although in the Estonian AI strategy's case the lacking competences related to AI means that Estonia finds itself in a similar position as Sweden. And the absence of the word “privacy” from the AI strategy could intuitively have inadvertently contributed to the problem of algorithmic trustworthiness not being guaranteed.

As such, the conspicuous absence of the words “privacy” and “growth” in the AI strategy document is an interesting contrast to the British and Swedish strategies. To the point the Digital Agenda document wound up acknowledging the absence. It is difficult to infer why this absence occurred, but one possible inference is that the AI strategy focused on AI uptake to the point where privacy concerns were not pointed out.

The Digital Agenda document mentions “privacy” four times and “growth” five times – “privacy” is one of the Digital Agenda's priorities, and the MKM states in the document: “We guarantee that people have the opportunity to manage the use of their personal data and protection of privacy.” (ibid p. 11) The much more direct use of privacy guarantees indicates that the Estonian political-parliamentary practice is itself setting itself up as the primary communicative force here – both through a content constraint and setting up a relation constraint where the political-parliamentary is itself determining that people – the public practice – have the ability to manage personal data use.

Although in the Digital Agenda's case, “economic growth” is only once used once, in a major contrast to the British and Swedish strategies which readily used “growth” as a shorthand for “economic growth”. Instead, the Digital Agenda readily applies “growth” in widely different contexts: from economic growth to growth in national security threats. (ibid p. 40) Which is indicative of how differently the Estonian political-parliamentary practice sees “growth”. So it begs the question of where the Estonian political-parliamentary practice diverged.

The Estonian system has its roots in the E-governance system and digital ID cards which were introduced in 2002. The impetus behind these has been a series of legal norms and laws that were passed in relatively rapid succession during the late 1990s and early 2000s. (Vassil 2016 p. 6)

Not only did Estonia thusly take more comprehensive steps at the same time as Wainwright v. Home Office was being decided upon and the Swedish Riksdag released its directive; these were integrated into the Estonian governance system earlier than Britain or Sweden began to seriously integrate AI into their respective governance systems:

“The digital ID project started already as early as in 1998 when Estonia had sought solutions on how to digitally identify their citizens. By 1999 a viable project in the form of current ID-card was proposed and the legal framework to enable digital identification was set up in the following years. In 2000 the Identity Documents Act and the Digital Signatures Act, the two most important bills regulating the use of digital ID’s, were passed in the parliament ” (ibid p. 7)

These laws primarily served to underpin further developments in e-governance; but they also served to establish e-governance as not only a political-parliamentary system but also a juridical-bureaucratic one. Akin to the Swedish example this can be interpreted as the Estonian government
being the primary driving force behind defining privacy and security in this context – but on a much more integrated context.

It is also interesting to note that the Estonian privacy regulations are directly enshrined in the Estonian constitution, with the 26th paragraph defining privacy in a manner reminiscent of Warren and Brandeis' definition:

“§ 26. Everyone is entitled to inviolability of his or her private and family life. Government agencies, local authorities, and their officials may not interfere with any person’s private or family life, except in the cases and pursuant to a procedure provided by law to protect public health, public morality, public order or the rights and freedoms of others, to prevent a criminal offence, or to apprehend the offender. ” (The Constitution of the Republic of Estonia 2015)

And the 43rd paragraph details privacy in messages – which extends to data sharing and AI usage because they fall under “commonly used means”:

“§ 43. Everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means. Derogations from this right may be made in the cases and pursuant to a procedure provided by law if they are authorised by a court and if they are necessary to prevent a criminal offence, or to ascertain the truth in a criminal case. ” (ibid)

The Estonian political-parliamentary practice not only sets up a content constraint by defining privacy and where exceptions are made, but also like the Swedish strategy focuses on crime fighting as a key exception. This has a significant effect on both the AI strategy and the Digital Agenda documents – particularly through the AI strategy's emphasis on data governance and the Digital Agenda's direct emphasis on privacy as a key cornerstone.

“The roles, responsibilities and tasks related to ensuring cyber security must be determined according to current needs and they must be comprehensive. Changes and growth in cyberthreats and additional tasks (certification, technology assessment, operational cooperation, etc.) have to be taken into consideration when updating the organisation of cyber security. ” (MKM 2021 p. 40)

In their efforts to deal with this, the Estonian government established an “X-Road” comprised of a decentralized network of interconnected services; that each have its own security service attached (ibid p. 24). This system is not only meant to mitigate the aforementioned risks, but also ensure that the internal security system is comprehensive across the governmental structure.

The “X-Road” is primarily concerned with establishing a “safer, quicker and more affordable system.” (ibid p. 6) This political-parliamentary solution effectively sets several constraints by doing this: in particular it sets a subject-centric constraint by ensuring that ordinary people and businesses alike do participate in the “X-Road” on the government's terms.

Since the MKM focuses on AI as a method to inform public and private activity the agency also plays a major role in shaping the Estonian stance. However, there is also an argument to be made that the MKM also responds to public activity, since it is ultimately working with the public on these matters.

Also, since Estonia has a significant Russian-speaking minority there have been some incentive to not let their domestic politics become a too significant geo-political issue. This is evidenced by an incident in 2007, when ethnic Russians brought down the internet for a month in protest to a statue
being removed from central Tallinn. (Karatzogianni et al. 2020 p. 118)

Not only did this event take place on both the streets and the Internet, it also had a long lasting if indirect effect on how the Estonian government sees crime fighting as a key exception to the privacy regimen.

This is a question that the Digital Agenda are concerned with, since it emphasises: “The consistent growth and development of cyber threats creates the need of rapidly developing our preventative capacity, and improving the monitoring and supervision of its implementation. “. (MKM 2021 p.43) This is worded in a vague manner – but one can argue that it is intentionally worded vaguely since the Estonian government likely have incidents like the riots and associated hacking attacks in mind.

The Estonian long term response was not to go for all-out censorship, instead they opted to further develop their internet and AI infrastructure by trying to combine an open internet infrastructure with a specialized threat management structure. Which is notable in both the AI strategy and the Digital Agenda: the former seeks to increase the availability of open data (KRATT – MKM 2021 p. 2) while the latter seeks to manage threats through:

“Cyber security tools supporting the monitoring of networks and information systems, the development of a situational picture and the management of incidents must be constantly updated and improved. ” (MKM 2021 p. 43)

Since the riot and assorted cyber-attacks were carried out in the arena of public discourse (chiefly around the statue removal) and not around the political-parliamentary or juridical-bureaucratic processes they essentially highlighted how the Estonian public practice can take on unconventional methods compared to the more formal document writing that the political-parliamentary and the juridical-bureaucratic practices use.

In this matter, those opposed to the statue removal directly challenged the subject constraint by protesting it – although one could certainly argue that the notion of challenging the subject constraint was undermined by the protests turning into a riot.

By contrast, since the Estonian government offered a carrot to the general public – in the form of platformizing citizenship – the political-parliamentary practice effectively strengthened the subject constraint on the wider public practice by relatively gentle terms.

This platforming continued by Estonia implementing GDPR later on. Estonia's implementation of GDPR is relatively similar to the Swedish implementation of the EU law, although it is also implemented under some relatively different conditions compared to the Swedish example. These conditions and the resulting implications on established Estonian laws and systems were not immediately clear, although the addition of the GDPR on top of the already existing Estonian law does imply that the political-parliamentary and juridical-bureaucratic systems.

Estonia's implementation of their AI strategy as such is heavily political-parliamentary on the whole, as evidenced by the significant weaving between the MKM and the government at large.

NPM is not entirely prolific within the Estonian system – contrary to British and Swedish responses. The private sector is included in the AI strategy and the Digital Agenda documents – for instance with the AI strategy focusing an entire category on the private sector - although it is evidently not the central feature. The reasons why are difficult to pin down conclusively, although
one potential reason for this may lay in how the Estonian government chose to structure its system. While the Estonian system has some similarities with the Swedish system it not only was established earlier, but it also was built with the idea of connecting the public practice with the political-parliamentary and juridical-bureaucratic practices.

In a manner this does allieviate Zuboff's central concerns to a degree – both documents alongside pre-existing efforts such as the X-Road represent a comprehensive effort to limit surveillance capitalism's reach and power to undermine the Estonian system.

However, there is one important caveat here in that the X-Road's structure does not necessarily prevent abuse by itself: in particular the risk still remains that surveillance capitalists do sign up for the Estonian service only for the surveillance capitalists to undermine the system from within and practically reject the discipline that the X-Road is supposed to dole out for them (Zuboff 2019 p. 128)

This is evident in both the AI strategy and the Digital Agenda documents – both of which concern themselves with the further development in the digital infrastructure. The latter acknowledges that the former has not taken privacy matters into account, and it did create some issues from the Digital Agenda. Which in turn also emphasises how privacy and AI measures are an ever-evolving field.

Regardless, by establishing a formal system through a relations-centric constraint the Estonian system sets would make it more difficult for surveillance capitalists to undermine the X-Road in theory. In order for surveillance capitalists to cultivate favours with politicians – as Zuboff fears – then surveillance capitalists would have to do more than to just cooperate in secret with the government organs such as the police.

The public practice does showcase some differences when it interacts with the Estonian government. Here the Estonian government's actions are largely held in response to what happens in the public arena – which is evident in the 2007 riot and its aftermath. While this interpretation focuses arguably too much on the public arena as a vector of change, it is worth noting that it also highlights how Estonian civic society differs from the British or Swedish counterparts.

"Some have argued that, within a relatively immature civic and media culture, Estonia has developed a unique form of ‘reversed’ censorship in which we not only see a very liberal media, but also a deliberate media effort to limit the any suggestion that there might be limits placed on the new-found freedom of expression. This ideology of a free expression is in part an expression of the power of the media that have been hostile to external criticism. One might also add that historians suspect that Sovietization during the Cold War was not as deep in Estonia as that witnessed in places like Belarus and the Ukraine.” (Karatzoganni et al. p. 118)

The public practice still influences the political-parliamentary and juridical-bureaucratic counterparts; not just because public events' aftereffects can spur action on the political level. Since the public are citizens under such a tightly integrated AI system – the E-governance model – the public are more directly connected to the political-parliamentary and juridical-bureaucratic processes surrounding AI.

It is also worth noting here that the riot and subsequent developments did not apparently shake the government's confidence in E-governance as a socio-political institution. On the contrary the Estonian government chose to solidify its structure both from a political-parliamentary standpoint as well as a public one.
How Estonia handles issues of privacy is thus heavily informed and influenced by existing laws as well as the state's relation to the public. This is to a large degree marked by the 2007 riot, but it nevertheless is a stark contrast to the British and Swedish examples where the interactions have mainly been confined to the buerocratic and the political domains.

The civil service and the juridical-bueracratic practice is the least visible in these interactions. Absence of evidence is not evidence of absence, but the relatively low key nature that the Estonian juridical-bueracratic system has taken in contrast to the British and Swedish system is notable.

6. 4. Comparing strategies:

The main unifying theme between the respective AI strategies is that all three are affected by the respective privacy legislation and how the practices use discursive practices. Privacy does not come up that often directly in AI strategies, but its presence – or absence - have significant indirect effects on how the AI strategies are worded. In particular, the AI strategies take care to not circumvene or otherwise undermine privacy legislation.

One notable instance is when the lack of discursive use affects an AI strategy is the Estonian AI strategy, which in turn lead to the Digital Agenda document having to aknowledge it. (MKM 2021 p. 14)

Both the British and Swedish political-parliamentary practices choose to rely more on NPM-centric solutions than the Estonian one in their respective AI strategies. However, while the Estonian political-parliamentary practice seeks to constrain corporations through the X-Road it still holds an open stance towards NPM-centric solutions - as evidenced by the AI strategy having a section dedicated towards private AI uptake - just less so than the other two.

While one can certainly argue which of the British and Swedish systems are more influenced by NPM, that question is rather ancilliary to the main point: that both the British and Swedish systems have intentionally chosen to embrace at least some aspects of NPM when privacy and AI strategies intersect. How do they do so differ: the British implementation of NPM leans moreso on the political-parliamentary level as evidenced by “multi-stakeholder fora” (UK Government 2021 p. 6), while the Swedish approach is more centralized around international cooperation and a framework-centric approach (Näringsdepartementet 2018 p. 8)

The British strategy is heavily reliant on the notion that the juridical-bueracratric processes set the precedent for the political-parliamentary system to implement the laws, whereas the Swedish and Estonian strategies are moreso leaning on the respective political-parliamentary practice communicating directly. This is notable not only since it diverges from the Swedish and Estonian responses, but also since it emphasises the role that privacy plays as a legal term – whereas in Sweden and Estonia those are defined by the respective political-parliamentary practices.

In particular the British protections to privacy have been allowed to evolve by the juridical-buecratic system, as the case of Wainwright v. Home Office proves by referring to past privacy cases. As such, on balance this is still a case where the juridical-buecratic structure has helped shape a strong privacy governance through the use of content constraints.

There is still room to doubt the British response's effectiveness in practice: not only due to the concerns presented by Drake et al, but also since the political-parliamentary response is being
heavily driven by a desire to at least appear as though they are differentiating themselves from the EU while also trying to assuage fears that they will not threaten privacy regulations in the process. This is a particularly important point given the already-low trust in technology amongst the British public. (Drake et al 2022 p, 275)

The challenges facing Sweden's government, meanwhile, is of a bit of a different matter since the lack of a public debate surrounding video surveillance: it has the potential to cause several issues related to privacy such as the education gap. For instance, if there is no debate regarding video surveillance it risks undermining public awareness regarding privacy questions. If this lack of debate extends to other areas of AI it also risks undermining confidence both when it comes to the political-parliamentary system as well as confidence in the Swedish system's ability to handle such questions.

The Swedish constraint system does to some extent alleviate this problem, though not entirely solve it. The IMY fining the Police is a case in point - since it is stopping a government agency from undermining the relation that the two have.

This is dependent on the IMY being an impartial force within the juridical-bureaucratic branch and that its politically mandated power is not undercut in the future – but it is still worth noting here since the political-parliamentary system has strengthened the privacy governance in its own way. The Swedish constraint system has a more clear political-parliamentary dominance than the British, with the juridical-bureaucratic serving as a notable enforcer.

The Estonian government appears the least NPM-influenced, albeit it still incorporates NPM-centric solutions into its “X-Road” schematic. The primary distinction between Estonia on one hand and Britain / Sweden on the other is that Estonia does not choose to model itself towards a straightforward NPM-centric solution: instead the Estonian government and political-parliamentary practice seeks to incorporate NPM solutions under its own system.

The interplay that exists between the political-parliamentary process and the public one is also notable here since it showcases that the Estonian public has been more active than their British and Swedish counterparts, even as the Estonian political-parliamentary practice evidently views the riot with a wary outlook (MKM 2021 p. 40).

Estonia's approach is heavily informed by the need for cohesion – as such, one can argue that Estonia's primary challenges lay within those confines. (ibid) While the long-term response to the riot can be argued as being well managed, the fact that the ID system is so heavily integrated into the government-mandated digital architecture does bring with it some risks in case those are hacked or otherwise manipulated.

On the other hand, the Estonian system is a product of the context it finds itself in: a small country with a significant minority population, a socio-political desire to embrace Western attitudes as well as a perceived need to connect the political-parliamentary practice with the public one. As such, one can make the argument that the Estonian system has one of the most comprehensive privacy governance and constraint systems, even as the AI strategy neglected to mention the word "privacy".

Through this it is possible to discern that the British constraint system is primarily set by the juridical-bureaucratic practice, while the Swedish system is more so leaning on a political-parliamentary primacy. The Estonian is also political-parliamentary but with a significant public
practice not seen in either Britain or Sweden.

Another area where the AI strategies show an interesting divergence is when it comes to the EU. The British AI strategy is heavily influenced by the British political-parliamentary practice's willingness to push away from the EU and create its own regulation in the form of the DPA, the Swedish strategy instead embraces international cooperation and is thus indirectly affected by the GDPR, and while the Estonian strategy also hews close to GDPR it is much more focused on building a national infrastructure.

**Conclusion:**

In conclusion, the most significant takeaway here is that the three countries' practices have independently contributed to the development and enforcement of privacy regulations – which in turn influences the AI strategies. While these practices' relative communicative activity do differ between the three countries studied and the practices have not behaved entirely independently of each other, the three countries' practices regardless showcased independence from each other when it came to constructing privacy regulations and affecting AI strategies.

However, that does come with the very important caveat that like Warren and Brandeis' time, the spur of innovation and the perceived need for more data is creating significant enough pressure on the states, the practices and the constraint systems.

The primary contribution this paper aims to have done is to prove that Björklund's and Zuboff's work on surveillance can be expanded to AI and privacy in general. In addition, the previous research also showcases that the AI strategies are worthy of scholarly attention.

This does have a few implications: while Björklund's and Zuboff's work has been mainly conducted within the field of surveillance, other forms of data management and transfer can also be explored under many of the same conditions. This is particularly relevant for not just surveillance capitalism, but also instances where the practices communicate with each other.

Fairclough's critical discourse analysis is also applicable in these cases. Communicative events as social practice helped to answer how and why the practices use speech to change privacy regulations and AI strategies. This has significant implications in a field where information sharing is an inevitability, especially as AI technology continues to develop.

This paper also have hoped to shed a light on how important it is for governments to have a strong privacy structure. It also has significant implications for combating possible overreach – not just by corporations or other non-governmental organizations, but also within governments themselves.

The application of NPM to a greater or lesser degree also shows that the path to a strong privacy structure can diverge on many points – for instance it can influence the practice that is most responsible for the privacy structure, as well as how and how much a government and its primary political practice cooperates with corporations.

These grey area cases – for instance, how closely the Swedish political-parliamentary practice adheres to NPM and how that affects the domestic AI strategy - remain areas of interest for future studies, not least since they are likely going to continue to factor in as long as socio-political and technological developments continue.
As far as AI itself is concerned, it is important to recall that the socio-political response to the technology's evolution and implementation does not only mean that the race itself is never-ending, but that AI's development can and will pose further privacy-related challenges. This is something that both the Clearview as well as riot exemplified, although it is worth noting that the strategies do encourage such development – with the aim to secure a better future.

As for avenues for future research: Can this type of study be applied onto countries with different democratic structures such as Japan and Taiwan? If this study is conducted through another author's interpretation of critical discourse analysis – such as van Djik's – then how much do the results change? Can this kind of study be applied to other new technological fields such as nanorobotics and genetic engineering?
Sources:

Published strategies, laws and documents:


E-Estonia, 2022: “Interoperability services: X-Road”, Estonian government, Tallinn


Information Communication Office, 2023: “Legislation we cover” London

Information Communication Office May 23rd 2022: “ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted” London


Journal articles and books:


**News articles and additional sources:**

Financial Times, 2020 “UK regulators warn banks on use of AI in loan applications ”, London


New York Times, 29th November 2021: “Clearview AI, a facial recognition company, is fined for breach of Britain’s privacy laws.“, New York


SVT, 11th February 2021: “Polisen får miljonböter för att ha använt ansiktsigenkänningsprogrammet Clearview.”, Stockholm