data to the people

Policy document
2020

Initiated by:
“Who determines the shape of technology, also determines the shape of our lives.”  - Marleen Stikker

Independence; that is what the internet was supposed to bring humanity. After all, everyone would have easy access to information and people could express their thoughts freely. The internet seemed to be the ideal environment for the ideal democracy with independence for all users. Unfortunately, we now know that that dream did not become reality. The internet has acquired a prominent place in society. But are we, the users, still in control of this internet and the data being generated within our information society? Or has that control passed to other parties, who thereby also determine the shape of our lives?

During our research, we discovered that much has already been written on the role of administration and policy within the digital society. Numerous studies have been conducted, the media discusses the role data play in our lives more frequently, and the debate is slowly entering the political arena. And a good thing, too, because the Netherlands are the sixth largest digital economy in the world. What stood out to us in this context is that there is little in the way of concrete policies regarding the ethical side of the digital society. Most studies conclude with an admonition aimed at politicians reminding them of the necessity of concrete policies with regards to data regulation. Politicians then respond saying they will get on top of it, but that more research and time are required because many uncertainties yet remain. In this way, they demonstrate a lack of appreciation for the urgency of this issue. And although the media is increasingly interested in the topic, it remains a complex subject on which only a small group of experts is well-informed. In short, many parties acknowledge the need for concrete policy measures, but no one is making the first step.

That is why we wrote Data to the People. In this policy document we focus on the ethical aspects surrounding the collection of data from individual internet users. In this document we first briefly outline the present situation with regards to our digital society. This outline gives an indication of its negative aspects, and enables us to propose concrete policy measures in order to improve the present situation. This policy document takes Dutch society as its starting point, within the context of the European Union, but the proposed policies are applicable to other countries as well.
In this way we hope to inspire policy-makers, politicians, and advisory boards with concrete policy proposals which elevate the discourse surrounding data. In addition to providing inspiration we are also happy to actively engage in conversation or discussion with interested parties in order to clarify and explain our analyses and proposals.
The three stages in the data route are the three pillars upon which our policies are founded: data transaction, data concentration, and data application. First, a data transaction takes place between the internet user and the data collector. The user parts with some of their data in exchange for a service. Next, there is an accumulation of data with the data collector, in other words a data concentration. Thirdly, there is data application. On the one hand, the data collector may keep the data to itself in order to optimise its services to the user. On the other hand, it may choose to sell the data to third parties for use in e.g. advertising.

This document is structured as follows. First, we present a fact sheet summarising the policy proposals. Next, we introduce the vision that informed the development of these policies. Finally, we discuss the three pillars of our policies. For each discussion, we adhere to the following structure: an outline of the present situation, the negative aspects of the present situation, an explanation of the proposed intervention, and an outline of the desired situation.
### DATA TO THE PEOPLE

<table>
<thead>
<tr>
<th>Present situation</th>
<th>Negative aspects</th>
<th>Policy interventions</th>
<th>Desired outcome</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users are protected by privacy laws such as the GDPR</td>
<td>Informing is a farce. Generalised descriptions and lacklustre enforcement offer only illusory transparency.</td>
<td>Better enforcement of the ability to correspond with data collectors Increase effectiveness of supervising agencies for more active control Reconsideration of data transactions that fall within the public domain</td>
<td>Meaningful transparency</td>
<td>Collective rather than an individual responsibility for protection of data transactions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destructive market power of data collectors</td>
<td>Data collectors are so large that there are no longer any alternatives. True value not accounted for.</td>
<td>Competition and data concentration: incorporating the value of data concentration in the market share test Competition and fundamental rights: the safeguarding of fundamental rights, such as privacy and equality, as a component of the market share test</td>
<td>No disproportionate market power for data collectors</td>
<td>Competition for high-quality data application rather than data possession.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data collectors have control over users’ data</td>
<td>Surveillance capitalism: the improper use of data (nudging, manipulation, misuse)</td>
<td>Research into the effects of differentiation in various domains Allow pricing and advertising on an aggregated rather than an individual level Define proper data application per domain and close off data routes</td>
<td>Users have collective control over their data</td>
<td>Users are protected from data applications which are deemed improper according to our public standards and values</td>
</tr>
</tbody>
</table>

---

*National ThinkTank*
Vision
Users of digital applications are currently insufficiently protected against the consequences of data collection. Thus, they become the unwitting victims of the actions of data collectors like commercial tech giants and the government. Public values such as privacy, equality, and autonomy are not protected online to the same degree that they are offline. That leads to dangerous situations both for the individual internet user and for society at large.

For this reason it is high time to create concrete policy that protects our public values in an online environment. This policy proposal is therefore founded upon two fundamental values: equal power relations and solidarity. These are the two values to which *Data to the People* is designed to contribute.

1. Above all, equal power relations must be enforced between internet users and large data collectors. The current skewed power relations between internet users and data collectors have created an illusory transparency towards the user. Privacy and cookie statements are a farce, because although they ostensibly inform the user, they do so in such a way as to be incomprehensible and undecipherable. Furthermore, the user often has no choice but to accept the terms because the online service is not available otherwise. This is problematic because unimpeded participation in the digital environment has become a fundamental component of our society. Power relations must be brought back into balance. Users have a right to meaningful transparency.

2. Secondly, it is important to better safeguard solidarity between users. Each user has an online profile that determines the content they get to see. This may cause users to become trapped in an online bubble, allowing their worldview to be manipulated. This is already happening in the form of (hyper)nudging, price differentiation, and advertising and website-contents tailored towards specific users. Thus, users are at risk of falling prey to discrimination and polarisation. This must be fought in order to safeguard solidarity between users.
Pillar 1

Data transaction
People give more and more data away to data collectors like Facebook, Google, and the government in exchange for products and services. At the same time, the users of these products and services have absolutely no idea what goes on behind the scenes. Who actually knows how much data they provide, what kind of data, or for what purpose? Yet data provide data collectors with a lot of knowledge about people and society at large.
Present situation

Users are currently protected by means of privacy laws such as the GDPR, the ePrivacy Directive, and other, sector-specific directives like the PSD2. These laws require businesses to fully inform the user about data collection and application in order to achieve transparency towards the user. In theory, the user should already be aware of the data they provide and what it is used for. After all, the GDPR sets a minimum for the information that users are required to receive in the form of terms of use. In practice, this transparency is illusory. Certainly, the GDPR has made strides with regards to protection of privacy and users have been, legally speaking, informed, but in a manner that is incomprehensible to anyone. They are presented with long-winded privacy and cookie statements in which the purposes of data application are formulated in broad or vague terms. Additionally, accepting cookies is presented as the only option for making use of online services and products. An inquiry by the National ThinkTank 2019 among the fifty most visited websites in the Netherlands revealed that only Google’s websites were entirely accessible without accepting any privacy or cookie statements.

Negative aspects of the current situation

Informing the user is, therefore, a farce! Demanding users to make an informed choice for every action performed online places a great burden on them. People tend to act intuitively. It cannot be expected of people to always act completely rationally. That could be seen in the financial sector, where people were, on paper, fully informed about risky products, yet still unable to oversee the consequences of their choices. In addition, there is another issue here which shows similarities with the financial sector: jargon. Privacy statements may be formulated in legally correct terms, but for that very reason they are impenetrable to laypersons. There are few people who can decipher the jargon employed here, if they even attempt to read it. This results in an information asymmetry; the user lacks information that the data collector is privy to. And even if they could read and understand all of it, they are often still left with no choice but to agree. Otherwise, they are locked out of the service. In short, current policies have created illusory transparency towards and autonomy of the user, which leaves no possibility for truly autonomous decision-making.

An apparent solution to increase transparency towards users is to expand the terms of use with all the available and specific information there is. But even though this would fully inform the user, it essentially means an expansion of the existing illusory transparency and does not address the issue. An even greater informational load would only intimidate people.

Desired outcome

The introduction of the interventions mentioned below would bring the digital society closer to meaningful transparency. The individual would no longer bear the personal responsibility to oversee the full consequences of each data transaction. Instead, there would be a collective protection against malicious use of data by data collectors. Additionally, public data would no longer disappear behind the closed doors of private parties, but can instead be put to better use for society.
Concrete policy interventions

In order to overcome the illusory transparency, we propose three policy interventions. As the above account shows, fully informing the user is not a practical solution. It is furthermore objectionable to hold people individually responsible for the protection of their own data, given their imbalanced power relation with the data collectors. That is why the aim of the interventions below is to accomplish a collective rather than an individual responsibility for the protection of data transactions.

Intervention 1: Better enforcement of the ability to correspond with data collectors

The current GDPR states that internet users have the right to, among other things, access to their data. This legislation is a step in the right direction, but does not go far enough, for the following reason: there is insufficient supervision regarding compliance. Hence, with many tech giants, it is unclear where you might file a request to access data, and sometimes personal information must first be submitted in order to request data. Once the request is successful and you receive your personal data, there is still the possibility that the data is incomprehensible. Complaining about this is difficult, because especially with foreign corporations, the complaints department is hard to reach and/or only available in English.

An example of the above is Twitter. After requesting our personal data we received a practically unreadable Javascript. Filing a complaint about this state of affairs is only possible through an online English-language contact form. Accessibility and clarity of services are commonly accepted values offline. This should also be the case online. For this reason, we advocate for comprehensible information on our data and accessible customer services of data collectors that store our data.

This responsibility also falls on (local) government. They must proactively inform citizens of the data they gather and use. Many people are unaware of how much or what kind of data they provide to the (local) government. Offering transparency in this regard would enable citizens to make meaningful contributions to the public debate on data collection.

Steps to be taken

• Improved enforcement of clear findability of the option to request personal data from data collectors through their own communication channels.

• This request should not only show which data the data collector has on the user, but also what the data collector uses it for. This information must be provided per request, and therefore tailored to individual users. A general privacy statement, as is currently required by the GDPR, is insufficient.

• The Data Protection Authority must enforce the rules more strictly for data collectors who provide the requested data past the legal term, in an incorrect form, or not at all.
Intervention 2: Increase effectiveness of supervising agencies for more active control

The ability of agencies which supervise matters of privacy to carry out their tasks is severely lacking. Research by Andersson Elffers Felix in 2017 already showed that the Dutch Data Protection Authority was too small for the extra responsibilities it acquired in 2018 after the introduction of the GDPR. The most likely scenario would require the watchdog to triple in size. In 2019, the Authority itself reported that it was unable to keep up with complaints. The insufficient capacity of the supervising agency undermines the functioning of current privacy law, and with it, user protection. The effectiveness of supervising agencies must be greatly increased in the short term. It is important to enable the Data Protection Authority to not only adequately respond to received complaints, but also actively look for violations. This has long been standard practice already in areas like food safety, so why not in the digital environment? Violations should furthermore be prosecuted so that judges will have to explain the current laws and regulations, so that improper use of data might be better punished.

Steps to be taken

• Enable the Data Protection Authority to adequately enforce regulations by increasing its current budget.
• Increase the Data Protection Authority’s effectiveness by expanding its workforce.
• The Data Protection Authority must look for violations more actively.
Intervention 3: Reconsideration of data transactions that fall within the public domain

Due to increasing digitalisation, private parties are intruding on the public domain via new channels. Clear boundaries between the public and private domains are blurred by the arrival of data collectors.

One example of this is found in education. Schools are receptive to the services offered to them by Google through Google Education. Schools receive free hardware and software, but in exchange they trade away data on their students. The education system is not necessarily improved by this, however. Student tracking systems may have advantages when it comes to watching a student's progress, but this data does not paint a complete picture of the student. Especially when the data is polluted or incomplete, it may lead to prejudice or discrimination. An increasing focus on data is therefore no guarantee of an increased quality of education. That the data furthermore ends up in the hands of a commercial private party is a worrying development.

It is furthermore important to answer the fundamental question: are we, as a society, allowed to relinquish students’ very personal data to private parties because schools themselves lack the financial means to have decent systems developed in-house? After all, these private parties serve their own interest first and foremost: the continued existence of the company and the profitability that requires. That is understandable, but we need to ask if that should also be allowed with data from the public domain and/or sensitive personal data such as student data. In the case of education it is therefore of the essence that schools develop a shared digital student system in the vein of Eduroam, which saw universities jointly develop a wifi network. That way, schools will benefit from the advantages of digitalisation without selling out the education system to a data collector.

Education is but one of the public sectors in which data collectors collect data for their own gain. There are other (semi-)public sectors where similarly intrusive admixtures of public and private technology have been realised. Examples of this are healthcare, unemployment benefits, the financial sectors (e.g. insurance companies), and the media. It is important that in these sectors, too, data is applied for the good of the public and does not disappear behind the closed doors of a handful of private parties. Hybrid forms could exist, such as public procurement or the offering of public services together with private alternatives. This is already the case with television channels. This way, the public Okuna and the private Facebook could enhance each other and raise their quality.

It is important to define what is covered by the public domain in order to then determine the extent to which private parties are allowed to collect data from the public domain. For once data is transferred to the private sector, it is usually no longer accessible to outsiders. An argument that is often made in favour of giving data to private collectors is that they are the source of innovation. That this is not necessarily the case has been shown in research by Mazzucato. Innovation may also come from the public domain. Moreover, it is part of the culture of public parties to prioritise public values during the innovation process. Private parties will weigh public values against private interests such as profitability. In education, for instance, the protection of students’ privacy may be of secondary concern to the revenue that could be generated on the basis of their data.

Steps to be taken

- Public sectors – such as education, healthcare, and police – must set directives for their own sector for the protection of public data within the sector.
- Public sectors should, with help from the government, invest more in their own data systems and software so that an alternative may be created for the free or inexpensive data systems of private parties.
Pillar 2
Data concentration
After the internet user carries out a data transaction, the data ends up in the hands of data collectors. The lion’s share of these data transactions are funneled towards a handful of very large tech giants such as Facebook and Google, but also with various government and government-affiliated organisations. This results in a large concentration of data in the hands of a small group of powerful actors.
Present situation

This large data concentration has led to data collectors having considerable and potentially destructive market power. They are able to buy out emerging companies, infiltrate other markets or sectors, and maintain their leading position through network effects (the effect that makes an infrastructure more profitable as the number of users increases). This frustrates healthy competition and sees the large data collectors becoming increasingly powerful.

Negative aspects of the current situation

Data concentration and the accompanying dominance of tech giants has several negative consequences for citizens and society at large. Firstly, it ensures that users will have no alternatives to digital services which collect data. Network effects have made it so that Facebook and Google are virtually inescapable. Furthermore, these companies have the capital to buy out other companies. Take e.g. the integration of Nest – a manufacturer of smart appliances like smoke detectors and thermostats – by Google. This allows Google to map exactly what you do at home. Emerging privacy-friendly alternatives that would arise in a perfect market are bought out or forced out. Not to mention the infiltration of other markets. Amazon is currently infiltrating the pharmaceutical industry. This allows it to collect data about its customers in different sectors and thus increase its dominant position through the possibility of linking data together. Where will this development lead in the future when data concentration and the market power of data collectors further increases relative to citizens and traditional companies? Data collectors will only acquire more data and more power. This leads to an impoverishment of the market and the disappearance of innovation due to the decrease in competition within the market.

Desired outcome

The proposed interventions in this pillar would drastically reduce the disproportionate market power of large data collectors. This would allow Europe to offer an alternative to both the American and Chinese model in which people are under constant surveillance in both the private and the public sphere. The European model is built on the fundamental rights of its citizens which also allows it to respond sustainably to future (technological) challenges.
Concrete policy interventions

The interventions outlined within this pillar are aimed at preventing, countering, or limiting this monopolistic market power by means of reforming competition law. A corporate takeover involves, among other things, a market share test, in which the market share is determined by the financial value of the corporation at that moment. This form of competition law does not work on large data collectors. For example: Facebook was able to take over Whatsapp with ease because Whatsapp was not worth much on paper. It was making relatively little profit, after all. As a consequence, data giant Facebook has managed to expand its power to a market with millions of users. This was made possible by the fact that the true value of Whatsapp, which is the millions of users’ worth of data it had at its disposal, was not accounted for in the market share test, and by the fact that the two companies are strictly speaking operating in different sectors. The activities of data collectors seem to be aimed at attaining a monopoly position. Therefore we seek to expand the market share test to include components that ensure that the market value indicated by the investigation corresponds better to the actual market value – i.e. including the value represented by data – and which provides more insight into the overlap between sectors. Because competition law is a mostly European affair, this policy should be implemented by the EU.

Intervention 1: Competition and data concentration: incorporating the value of data concentration in the market share test

In the age of surveillance capitalism – “a new form of information capitalism [that, red.] aims to predict and modify human behavior as a means to produce revenue and market control” – having access to data is of great value. Data concentration should therefore be a component of the market share test. When corporations already possess large amounts of data separately, this data concentration only grows after a merger or takeover. When this data concentration leads to disproportionate market power, a takeover must be prevented. Whether or not the corporations are operating in different sectors is not relevant to this matter. Data concentration is all the more lucrative when data from different sectors is combined. There are already several policy initiatives proposing similar solutions, but these proposals are not treated urgently enough in (international) politics. This allows large data collectors to remain one step ahead.

Steps to be taken

- Add the criterion of data concentration to market share tests within competition law on a European level.
- Process existing proposals with regards to data concentration and competition law with urgency in (international) politics.
Intervention 2: Competition and fundamental rights: the safeguarding of fundamental rights, such as privacy and equality, as a component of the market share test

Though European – and therefore also Dutch – competition law is currently largely concerned with economics, it originated from the idea that the principles of free markets and democracy are linked. Because competition law is focused on consumer welfare, the balance between corporations’ economical and non-economical interests has been skewed. This becomes especially clear when data collection takes place on the borderline between the private and public spheres, such as in education, the media, and the insurance industry, because competition law and its exceptions assume a strict boundary between private and public spheres.20

This balance between the public and the private needs to be reinstated. EU-treaties not only allow for such a reconstitution of competition law; it is also in accordance with the EU’s goal of creating a social market economy. It is therefore imperative that multiple values are accounted for within competition law, such as sustainability, solidarity, democracy, etc.21

Continuing to add components to market share tests that express the value of corporations in their current form is not a sustainable solution. In the future, new (disruptive) technologies could create new market powers. In order to keep up with the increasingly changing and complex world around us, it is necessary to include the safeguarding of fundamental rights in market share tests. That way, there would be no need to choose between consumer welfare and concerns like privacy and prosperity, because all aspects would be included in the decision.

Step to be taken

- Reform competition law to have public values as its fundamental principle to prevent data collectors from acquiring too great a market power.
Pillar 3
Data application
As soon as data collectors have the data in their possession, there are roughly two ways in which they can apply it. They can use the data to optimise their services and products, or they can sell it to external parties for e.g. advertising revenue. These two applications of data do not only involve personal data, but also data that is generated by the way users interact with a platform: the exhaust data. This exhaust data provides a lot of insight into how people behave and is therefore of great value. The application of both personal and exhaust data can have far-reaching implications for our society.
Present situation

Currently, a data collector, after a data transaction has taken place between the internet user and the data collector, has control over this person’s data. They are free to apply personal data for the purposes outlined within their own privacy statements. However, these purposes are often formulated in broad, general terms. This leads to ambiguous situations and an illusory transparency which enables data collectors to utilise data as they see fit. They may pass on the data to a third party whilst providing no accountability for this third party’s activities. This means there is no oversight on what exactly happens to an individual user’s data. The lack of public debate concerning the application of data furthermore shows that the topic is low on politicians’ lists of priorities.

Negative aspects of the current situation

Legally speaking, an individual has no property rights to their own data. These rights are difficult to regulate for, due to all manner of technological issues such as the copiability of data and the fact that a lot of data is generated within a corporate context. Nevertheless, we are reaching a point where people have lost all control over their data and corporations are free to continue their aforementioned surveillance capitalism unimpeded. They will skim off the top of consumer welfare by gathering consumers’ data and applying it to the improvement of their products and services or by selling it to third parties.22 Downsides of this revenue model include differentiation, nudging, and manipulation of internet users.

 Desired outcome

We are collectively protected and no longer bear full individual responsibility to secure our data or ensure that we have read every statement. People have regained some control over their data, the basis of collective and widely supported measures.
Concrete policy interventions

With our interventions we seek to protect the user against improper data application. In order to achieve this, responsibility for the data transaction should no longer lie with the consumer and improper use of data should be regulated per sector (e.g. insurance industry, healthcare, etc.). This collective form of protection offers a counterbalance to the unequal power relation between data collectors and users. Additionally, societal cohesion would be safeguarded by limiting differentiation, nudging, and manipulation.

Intervention 1: Research into the effects of differentiation in various domains

The collecting and application of data has different effects in every sector. However, these effects are currently largely unknown. There are fears that detailed differentiation based on data could have negative consequences for the principle of solidarity which underpins insurances. There are also concerns for a potentially increased inequality of opportunity in education due to prejudices which arise from (low quality) data. The financial sector, police and justice departments, healthcare, politics, journalism and media, all show signs of the negative impact of hyper-differentiation upon our society.

More research is therefore needed into the negative effects of differentiation on the basis of big data in these vulnerable domains. Such studies have barely been conducted within or about the Netherlands. Our proposal is to focus research on the consequences of differentiation on equality within our society. These studies should include within their conclusions concrete proposals regarding the permissible extent of differentiation within the sector in question. These proposals could take into consideration the advantages offered by differentiation to the data collector and the interests of the user. A fair power relation should always be the guiding principle in these considerations.

Step to be taken

- Research into the effects of differentiation in various domains (such as healthcare, education, and insurances) by an independent organisation such as the Rathenau institute. On the basis of this research, directives could be established per sector regarding the application of differentiation and the ensuing effects.
Differentiation, for example in pricing, advertising, or content that is provided, could lead to discrimination. Anti-discrimination law is supposed to protect against differentiation, but is inadequately enforced within the digital domain. Furthermore, the ability to differentiate is much more advanced than it used to be. Consider, for example, the ability of algorithms to detect characteristics other than those protected under anti-discrimination law (such as income) to differentiate or discriminate by.

There are many arguments to be made as to why advanced differentiation is unethical. Firstly, the quality of data is too flawed to accurately apply micro-differentiation. Differentiation could therefore be erroneous, which could have major consequences for those affected. Furthermore, the assertion that differentiation increases prosperity does not fly here. There is indeed an increase in prosperity, but only among corporations rather than consumers. Additionally, a majority of the Dutch population considers pricing discrimination to be unacceptable. The possibilities afforded by hyper-differentiation are not yet fully exploited by large data collectors, but there is little preventing them from doing so in the future.

Our proposal is to put a limit on differentiation, or in other words, a stop to hyper-differentiation. Differentiation should then only be allowed up to the aggregate level of e.g. 1000 people who share similar characteristics, not on an individual level. The permissible degree of differentiation should be considered per domain. New services such as DuckDuckGo demonstrate that a revenue model may be built around aggregated differentiation as well.

**Step to be taken**

- Set a limit to differentiation per domain to prevent hyper-differentiation.
Intervention 3: Define proper data application per domain and close off data routes

Now is the time to conduct studies into the proper application of data per domain and devise policy based on the results. The aim here is to reduce or prevent the effects of differentiation, nudging, or manipulation. A possible example of this could be that data about individuals or groups within a certain domain cannot be applied within another domain. We could, for instance, close off the potential data route from Facebook to insurance companies. This would entail prohibiting insurance companies from using data generated by other platforms. It should be noted that “data” is not referred to in the narrow sense, here (i.e. personal data). In order to offer adequate protection, exhaust data must be included in the definition.

It is furthermore high time for a public debate about which forms of data application are (for the time being) ethical or not. Researchers Moerel and Prins bring up the examples of individual genetic information, or insurers who calculate premiums based on individual lifestyle or even driving style. That this is not merely a hypothetical issue is demonstrated by initiatives from ASR Vitality, which are already being advertised in the Netherlands. This app promotes a healthier lifestyle and offers discounts on additional insurance if progress is made within the app. The fact that ASR Vitality is a separate legal entity from insurance company ASR – and thereby guarantees that no data is being shared with the insurer – does not mean we should not err on the side of caution. There are already several examples abroad of data platforms sharing their data with insurance companies.

Another way to ensure proper data application is by instituting a new legal test as the basis of protection of privacy. This test, proposed by Moerel and Prins, takes into account not only the interests of the individual, but of society as well. The test offers a replacement of all rights described in the GDPR – such as the right to access to one’s data, rectification, permission, and removal of data – by incorporating them into a comprehensive “legitimate interest test”. The “legitimate interest test” takes all relevant interests into consideration. “[The test is] a contextual analysis that takes various factors into consideration, including the nature of the data that are processed (sensitive or not), how the data is processed (does it involve large amounts of data? Are the data combined with other data?), the reasonable expectations of the person whose data are being processed, the status of the data controller and the individual involved and their respective positions of power, and also the measures that the data controller has taken to reduce the impact on the privacy of the individuals concerned, such as data minimization and technical measures such as encryption and pseudonymization”. A judge will be able to decide from this test whether legal action is required. For example, the test would ensure that permission by an individual to be subjected to misleading advertising would be inherently unlawful. This would create meaningful control over data.

Steps to be taken

- Close off sensitive data routes through legislation and regulation.
- Create a public debate regarding forms of unethical data application. This requires cooperation between (local) government, politics, research institutes, and the media.
- Reform privacy law by instituting a “justified interest-test”.

National ThinkTank
Conclusion
There is work to be done! As a society we face the great challenge of taking digitalisation in the right direction. If we counter the current unequal power relations and maintain solidarity between us, digitalisation has the potential to improve everyone’s lives. No one will claim this task is easy, but it is vital in order to guarantee a safe future for the Netherlands and Europe. Only then will citizens be able to make use of the internet freely and safely in the future, and of all the advantages it brings.

As a society, we therefore need policy makers, politicians, and advisory councils who will not shrink from substantial measures and who will rise to this challenge in unison. We have put forth many concrete interventions in this policy document in order to shape this secure and fair digital society more concretely. The realisation of these interventions requires policy makers, politicians, and advisory councils to cooperate, with each other as well as with society.

We hope that this policy document will be of help in this matter. We, Elsbeth and Sem, would be more than happy to contact you and brainstorm with you about the desired forms and effects of these interventions in your environment.

**Acknowledgements**

This policy document is the result of a desire for a fair digital society and is founded upon many hours of research, interviews conducted with experts, and interviews with people on the street. We extend our thanks to the National ThinkTank and all its (thematic) partners.
Appendix

3. Vanwege de leesbaarheid van dit document is ervoor gekozen om enkel de hij-vorm te gebruiken. In alle gevallen kan er echter ook de zij-vorm ingepast worden.
7. In its analysis, the National ThinkTank has requested participant data from fifty websites. Four websites provided the data in unreadable form. Additionally, there were several websites which did not respond at all, or provided inadequate information.
8. Liesbet van Zoonen, Emiel Rijshouwer et. al. (2019). Jouw buurt, jouw data. Uitkomsten van de onderzoeksgame over kennis, houding en gedrag van burgers in de slimme stad. 16-17
11. Okuna is a social network which takes ethical values as its point of departure. The initiative is currently in the testing phase.
13. From this point onward, this pillar discusses commercial organisations, unless otherwise indicated.
Colophon

The policy document Data to the People was written by Elsbeth and Sem as part of their participation in the National ThinkTank 2019 (Dutch: De Nationale DenkTank, NDT19). The main question of the NDT19 was: how can we realise a digital society that is healthy, resilient, inclusive, and fair? This topic was explored by twenty young academics. Data to the People is one of the ten solutions devised by the NDT19.

Do you have any questions or remarks in response to this document? Or would you like to know more about its authors or the National ThinkTank? Please feel free to contact us.

Authors:

Elsbeth van den Hazel
e.vandenhazel@nationale-denktank.nl

Sem Nouws
s.nouws@nationale-denktank.nl

Design: Hella Hekkelman (lay-out), Saiid & Smale (font title page)

Translation (from Dutch): Gwan Brandhorst

Photography: p. 6-7: Nejc Kosir; p. 26-27: Niels Gilissen