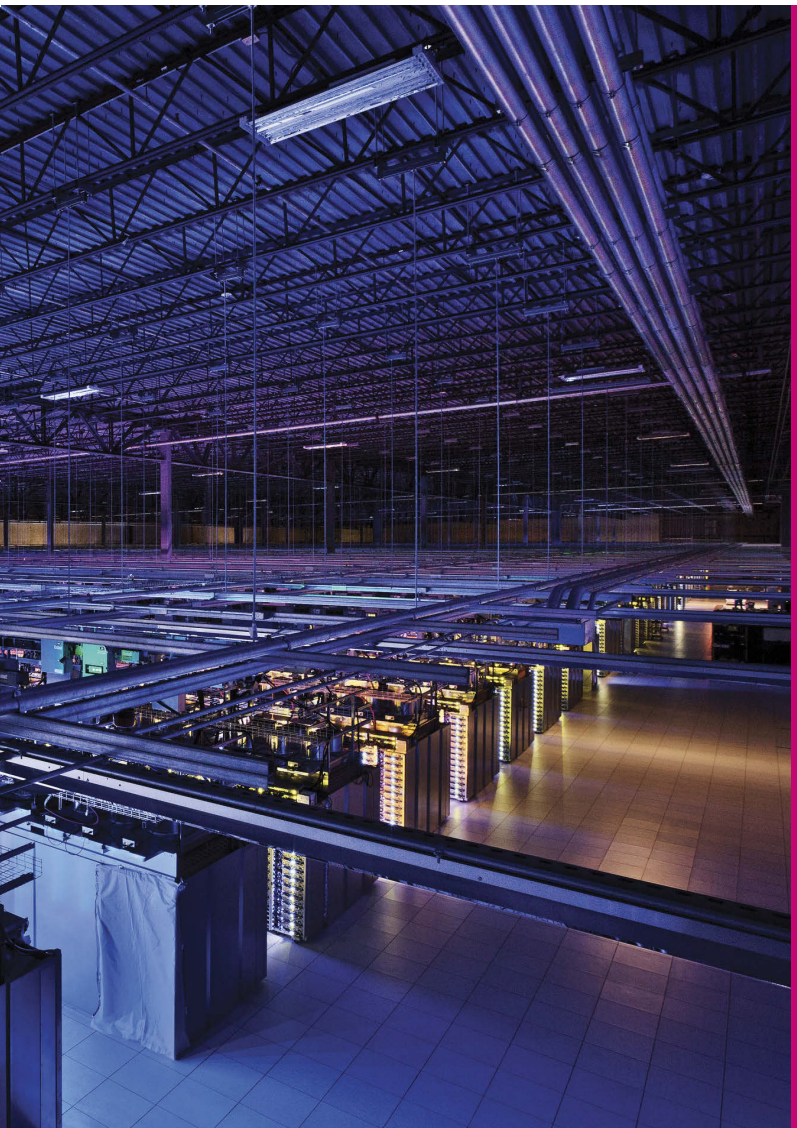
CPB Netherlands Bureau for Economic Policy Analysis

Expanded choice for citizens | *More room for businesses*



CPB Policy Brief | 2014/04

Choosing privacy

How to improve the market for personal data

Michiel Bijlsma
Bas Straathof
Gijsbert Zwart

Summary

Businesses and the government are all collecting more and more personal data, and they use these data ever more intensively. This is mostly to the benefit of citizens, but not in all cases. Opinions about privacy vary greatly, and businesses use personal data in various ways. Weighing the pros and cons, therefore, is something that can best be done by the parties involved. Innovative use of personal data is stimulated by an increased freedom of choice for citizens and businesses, with people determining their own level of privacy. Having a market for the user rights of personal data allows citizens and businesses to make these choices.

Without government policy, the market for personal data cannot function properly in practice. For example, it is difficult to monitor how businesses use data, and drafting tailor-made privacy agreements between businesses and customers is costly. Enhancing trust is an important objective of the Dutch Cabinet.[1] The work by the supervisory body, the Dutch Data Protection Authority (College Bescherming Persoonsgegevens, CBP), is crucial in this respect. However, in addition to trust, this also requires sufficient scope for making various choices and for entrepreneurship. This policy brief considers a number of related policy options. These options concern the right to erasure, the specifications of privacy agreements, use of personal data without permission, European supervision, certification, and technology that provides citizens with more control over their personal data.

[1] Letter Cabinet vision on e-privacy: *towards justified trust* (Naar gerechtvaardigd vertrouwen), 24 May 2013.

1. Introduction

In June 2013, Edward Snowden sent tens of thousands of classified documents of the US National Security Agency (NSA) to various newspapers. Snowden's disclosures showed that security agencies were collecting a larger amount of personal data than experts had previously thought possible[2], and also made citizens more aware of the large amounts of their personal data that are in the hands of third parties. Why would the NSA be the only party with this type of information? Developments in information and communication technology and the internet itself cause a rapidly growing mass of data that can be traced back to individual people. What do large online companies, such as Google, Amazon or Facebook, as well as the more traditional companies (e.g. banks and supermarkets) really know about us? Technological progress induces a continuing discussion on privacy.

The privacy discussion has been held along two – not necessarily mutually exclusive – lines, for decades. On the one hand, there is the legal approach with the respect for people's personal lives enshrined in the constitution. Under this approach, according to its followers, privacy agreements must state the exact purpose for which data are to be used. On the other hand, there is the economic approach to privacy that centres around the various options for shaping the personal data user rights. The fundamental attitude here is that people are free to manage their personal data as they see fit.

The separation between the two approaches is also a geographical one; the general legal approach is taken in the European Union, whereas in the United States there is more room for the economic approach. The European Data Protection Directive of 1995[3] and the recent proposal to regulate data protection[4] both emphasise citizens' rights.[5] The United States have no generic privacy laws; such laws may vary per state, and the interests of businesses play a larger role. The Federal Trade Commission (FTC), however, does enforce sector-specific regulations on privacy.[6] Companies formulate a privacy policy and operate on the basis of *notice and consent*, which means that consumers are asked explicitly to agree to company policy. The sale and publication of data may even fall under the First Amendment: the right to freedom of speech.

This policy brief studies whether the EU and US approaches could be united, for an economic approach of the costs and benefits of privacy policy, including its important role in the marketability of personal data, does not exclude the constitutional right to privacy.[7] A legal approach also requires that choices are made about the specifications of privacy policy, with a role for economic arguments.[8]

Privacy laws can have a large impact on welfare. If privacy is too tightly regulated it may harm citizens; for instance, when business innovations are restricted too much. The use of Big Data – in this case, the seeking of new applications for already collected personal data – would then be

[2] Bruce Schneier, een vooraanstaande expert op het gebied van cybersecurity en in het bezit van documenten van Snowden, blogde een tijd lang iedere week over een andere, onbekende techniek van de NSA (www.schneier.com).
[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[4] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[5] The draft regulation currently before the European Council will further enhance these rights.
[6] The Federal Trade Commission (FTC) enforces a number of privacy regulations, such as the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act, CAN-SPAM Act, Health Insurance Portability and Accountability Act, and the Privacy Rule of the Telemarketing and Consumer Fraud and Abuse Prevention Act.
[7] When privacy is a constitutional right, personal data can also be marketable. In this respect, it must be noted that there considerations of privacy may differ. It can be seen as synonymous with confidentiality of personal data, but may also be regarded as the *option* of confidentiality of personal data. In case of the latter, voluntarily sharing personal data puts no limitation on privacy .
[8] For example, the span of purpose limitation.

close to prohibited. However, too little regulation may also be harmful if it enables companies to use such information without the individual's prior knowledge or consent for purposes that could harm those concerned. Or, if data are used for purposes other than those approved.

2. The value of personal data and the privacy paradox

US telecommunications company AT&T offers a subscription to its glass fibre network in Austin, Texas, for USD 99 per month. However, customers can also choose a subscription of only USD 70 per month, but then they must agree to AT&T using the data on their internet surfing behaviour to present them with customer-specific offers and advertisements.[9] This example illustrates the fact that personal data are of economic value to companies. In itself, this is nothing new. What is new is the scale on which businesses collect, save, combine and analyse such data and the related economic value. Thus, the market capitalisation of companies such as Google and Facebook now is comparable to that of giants such as Exxon and Walmart.

Personal data are generated more or less continuously; whenever people use social networks or search engines, when cookies collect and forward information on their internet surfing behaviour, when apps on mobile phones register and pass on user locations and phone usage, when supermarkets monitor the types of products that are being bought, when health care suppliers register the use of health care services, when recorded images taken in public spaces are being stored, or when payments are made by bank card.

Information on individual people represents value to businesses in various ways. It enables businesses to better gear supply to demand; it means they can identify potential customers and direct specific advertising to the needs of those customers. This enhances the chances of people receiving appropriate offers, in turn, leading to an increase in the yield per advertisement for those businesses. In addition, businesses may use personal data to manage risks. For example, having more information on people's payment behaviour enables a better estimation of the risk of defaults when issuing credit. Furthermore, being able to cross-reference customer information using alternative data sources also reduces the chances of fraud, and, lastly, by identifying trends in demand, companies can improve their stock management.

Having more detailed information on potential and existing customers also enables companies to increase prices when customers would have a higher willingness to pay for a certain product. Insurance companies, for example, could demand a higher amount in premium from high-risk customers than from other customers who pose a lower risk. This type of price discrimination enables better attunement between demand and supply, which in turn adds to more efficient market results, although this also and inevitably disadvantages certain customers.

Finally, businesses may use personal data to develop new products. Professional social networks, such as LinkedIn, offer new possibilities to those who seek employment as well as to companies looking for staff.[10] Internet search engines use their customers' previous searches to perfect their algorithms. Phone and twitter behaviour provides information on traffic jams and is used for crowd management at large events. Businesses are monitoring Facebook and Twitter to measure customer satisfaction levels. E-health applications enable people to monitor or diagnose their own physical health.

[9] http://arstechnica.com/information-technology/2013/12/att-offers-gigabit-internet-discount-in-exchange-for-your-web-history/
[10] With implication for labour market efficiency; for example, see Van den Berg (2006).

Many people, however, have an ingrained feeling of unease about strangers gaining access to their personal information. The overall majority of internet users in the United States say they are at ease with their behaviour being monitored on the websites they visit (Turow et al., 2009), although it does depend on what that information is subsequently used for. When surfing behaviour would, for example, be used for short-term discount offers, this is more acceptable to a large number of people than if it would be used for advertisements. Uneasiness can also be a reflection of the risk of actual damage. This damage may be caused by the particular company entrusted with the data, but also by third parties due to data having been resold or lost. When people think that there is a good chance of falling victim to fraud or theft after leaving their address or credit card details, they will be less inclined to make online purchases. In addition, people may incur damage if certain specific characteristics are made public. Employers, for example, are less likely to hire women if these women are pregnant at that time. Another example is that of people who have been involved in traffic incidents having to pay a higher insurance premium.

This feeling of unease is in stark contrast to the ease with which people sometimes provide their personal data. Many agree to privacy agreements without knowing the content of those agreements. On Facebook, some people share every detail of their private lives, and it has been nearly fully accepted that Google reads the emails of gmail users. This points to a privacy paradox.

This gap between people's concern over privacy according to public opinion and the value they award to their privacy in everyday practice also is apparent from empirical research. Consumers who fear an invasion of their privacy appear willing to part with their personal data for any small amount of money. Experiments with purchase decisions have shown that many consumers have no problem to share their personal information with the salesperson, even when this could have easily been avoided.[11] The recent social unrest about the ING Bank also fits this paradox; although the ING's plans are only modest, compared to the usage of personal data by Google, Facebook and a variety of mobile phone apps, such as the popular Whatsapp.[12]

3. The personal data market

One possible explanation for the privacy paradox is the rather large differences in the value that people place on their personal information. Businesses also vary in the value they award to those data. Large enterprises that already have collected large amounts of personal data are able to deduce more information from new personal data than companies that only have a small amount of data already at their disposal. A marketable user right for personal data could do justice to the large variety of situations and preferences.

In an economically ideal world, businesses would only be allowed to use personal data if the total benefits would outweigh the total cost. If they do not, it would in fact be preferable not to use the data. As it would be impossible for the government to determine this balance for every individual case, it stands to reason that people and businesses would be allowed to make this judgement for themselves.

If people are able to give their consent about the use of their personal data for a specific purpose, they can weight the benefits of this use against the costs. Consent is then provided not only when

[11] Grossklags and Acquisti (2005).

an individual has a direct personal benefit from a company using his or her data, but also in cases of adequate compensation being provided to counter the disadvantages.

From the perspective of consumers, this compensation may be a discount in price, or a free service or direct payment. In such cases, there is an exchange; user rights to personal data are exchanged for valuable products, services or financial compensation. In this way, the advantages and disadvantages of the use of personal data can be weighed against each other, per case.

This, however, does require that user rights are put in writing, so that both the data provider (the person) and the user (the company) can negotiate the conditions of this use. Without transferable user rights there would only be a 'one size fits all' solution – one that does not take individual preferences into account. This would also frustrate any data use that would benefit both parties.

Most goods and services are easy to trade, including data such as on personal information. A particular characteristic of data is that multiple parties are able to use it. Therefore, it is not the data themselves that are being traded, but the rights to their use. This enables the owner to detach the personal data from their use by others, which prevents unwanted use.

In privacy agreements, the user rights to personal data are being traded. There are also other examples of user rights enabling the trade in information, such as in the case of patents. A patent enables an inventor to divulge his invention to potential buyers without diminishing the value of his invention. In this way, businesses are drawn to invest in innovation, even if they cannot directly achieve the benefits from such innovations themselves.

Tradable user rights also form the solution to other issues of immaterial goods distribution. For example, New Zealand fisheries have worked with tradable fishing quotas since 1986.[13] In order to protect fish stocks, a limit has been placed on the catch of various fish species. The tradability of these fish quotas enables efficient fishing businesses to acquire rights from less efficient colleagues. Here, both parties benefit; the buyer is able to catch more fish and the user is better off receiving a payment for his fish quota than he would be with the profits from using the quota himself. In addition, society also benefits when saving takes place where it can be achieved against the lowest cost.

Through the user rights to personal data, privacy regulation is able to take into account the possibility of different people and businesses awarding a different value to the sharing of such data. If individuals can determine for themselves how and under what circumstances their data may be used, this could generate transactions that would be of the highest mutual benefit. In theory, that is; but does it work like this in actual practice?

4. When does the market fail?

In practice, the market fails quite regularly; the personal data market either does not function well or transactions fail to take place at all. For example, it is not easy and rather costly to draft contracts on an individual basis. Moreover, it is difficult to check how businesses and the government handle personal data, and whether individuals provide truly accurate data themselves. In addition, citizens are not always able to decide what would be best for them.

Transaction costs prevent the drafting of specific agreements that are attuned to an individual and/or a particular situation. It takes time and effort for consumers to become familiar with the privacy policy of each company; the reading of all privacy agreements alone would cost the average US citizen around 200 hours per year (Campbell et al., 2013) and for most readers would not result in them understanding these agreements (McDonald et al., 2009). Negotiating a custom-made agreement is impossible for most consumers, and such negotiations are also likely to fail due to differences in opinion about the value of personal data. Therefore, user rights should be standardised in such a way that deviations from this standard mostly are not needed in order to achieve a more efficient distribution of rights.[14] There are also differences in the negotiating positions of companies and private citizens. It is more difficult for consumers to avoid the internet giants than it is to deal with companies that compete heavily for consumer attention.[15] After all, competition also disciplines the privacy policies of those companies. In addition, different product suppliers may distinguish themselves in the way in which they collect personal data. This also leaves consumers with a wider range of choice.

Another issue is that of moral hazard. Individual consumers are hardly able to check whether a certain company has complied with the agreed use. And even if customers are aware of data losses or unauthorised use of their personal data, it is very difficult to claim any damages. This also applies to government authorities – the other group of collectors of large amounts of personal data; for example, for the purpose of more efficient taxation or for combating crime. Cases such as the recent NSA affair illustrate that authorities sometimes also cross the line. Even if data were collected with the best of intentions, they could still end up in the wrong hands by accident or as a result of criminal hacking. Online auctioneer Ebay was brought into discredit, recently, when data leakage provided outside access to the personal data of possibly 145 million of its users.[16] And in the Netherlands, the DigiNotar affair[17] showed that also the transfer of personal data to the government is not without the risk of leakage. Citizens and consumers depend of the care with which businesses and government handle their personal data. They are unable to check the level of care for themselves.

To overcome this moral hazard, consumers in actual practice depend on the reputations of companies and governments, as well as on the public enforcement of agreements and safety standards by supervising bodies, such as the Dutch Data Protection Authority. Having a good reputation is useful only if losing it causes damage to a company. Outside supervision works only if the conditions under which personal data may be used are standardised to a certain degree. If every consumer enters into a custom-made privacy agreement with their internet provider, it becomes too complicated for a supervisory body to verify, on their behalf, whether providers have been complying with those agreements.

A third barrier to an efficient market for personal data is the fact that *freedom of choice* assumes that citizens are able to decide what is in their own best interest. In practice, people are only able to make such decisions to a limited degree, or they decide not to study the details of their choices. Choices depend, for example, on the way in which something is presented. Furthermore, people often are unable to oversee all the consequences of their choices or include these in the

[14] Standardisation of privacy agreements may also help to make people more aware of the content of these agreements, as Kelley et al. (2010) show in an experiment with more user-friendly privacy information on terms and conditions.
[15] Such powerful market intermediaries also cream off part of the value of data transfers to advertisers and businesses, which hinders efficient transactions. Also see Athey (2014).
[16] http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521
[17] This Dutch company handled security certificates for various government services. After they were hacked and following criticism of the company's safety procedures, the government stopped working with this service in 2011.

decision-making process. They also may be insufficiently aware of any long-term consequences related to their decisions. When asked[18] who they think has access to their credit card data following an online purchase, only a small minority of people considers the possibility of hackers also having access, and some forget that their bank has knowledge of the transaction, as well. Privacy policy, therefore, serves to protect citizens against substantial damage from taking the wrong decisions.

Having the freedom to issue user rights to personal data does justice to individual choices and preferences. However, unbridled freedom does not appear to achieve optimal results. The question, thus, is how privacy policy could unite these two worlds, and how regulation could leave sufficient scope for individual preferences and personal situations, while protecting citizens from market shortcomings.

5. Policy options

In the Netherlands, the Dutch Data Protection Act, together with the EU Directive, places the user rights to personal data mostly in the hands of individuals themselves. Furthermore, most conditions under which personal data may be used have been stipulated and, thus, contracts have been standardised to a large degree. There are few possibilities, for individuals and companies alike, to deviate from these legally regulated standard contracts. The new European privacy regulation[19] increases the rights of the individual even further; among other things, by applying the 'right to erasure' also to data that are being used fully in compliance with privacy agreements.[20] This more stringent privacy policy, with emphasis on legal protection, may reduce the chances of undesired use of personal data. At the same time, it limits the possibilities for the types of use of personal data that individual citizens would not object to. As described above, this leads to social costs. Government could improve the functioning of the failing market for personal data in four ways:

- by clearly establishing user rights and their transference;
- by lowering transaction costs;
- by combating moral hazards;
- by overcoming the undesirable consequences of limited consumer rationality.

Below, six adjustments to current policy (including the new privacy regulation) are presented to help achieve the secondary objectives above.

Policy option 1. Adjustment to the right to erasure

When a citizen exercises the right to delete data that has been rightfully acquired and used, the business concerned should be entitled to compensation that has been established in advance.

Dutch citizens already have the right to know which of their personal data are registered.[21] They also have the right to correct, supplement or delete such data, but only if the data are incorrect, incomplete or unnecessary for the intended use.[22] The right to correct, thus, cannot simply be applied by citizens in an attempt to conceal negative personal information, nor can it be used to

[18] in the study by Acquisti and Grossklags (2005)
[19] The European Parliament has agreed, after adjustments, to a proposal for personal data protection submitted by the European Commission. At the time of publication of this study, the proposal was still before the European Council.
[20] Initially, the 'right to be forgotten' was proposed, which was even more far-reaching.
[21] Article 35 (Dutch Personal Data Protection Act (Wbp)).
[22] Article 36 (Dutch Personal Data Protection Act (Wbp)).

one-sidedly terminate a privacy agreement. The proposed European regulation on data protection takes this one step further. Under the current proposal, citizens will have the right to delete data – even if they had previously given their explicit consent for the use of that data.[23] This right to erasure provides citizens with the possibility of correcting their mistakes and offers them a greater degree of control over the use of their personal information. This may increase people's willingness to share their personal data with others.

The elaborate right to erasure also has a disadvantage; it diminishes citizens' credibility in entering into an agreement on the use of their personal data. This may disrupt the functioning of the personal data market. For businesses, the right to erasure means that personal data become less valuable – as purchased user rights may be taken away without grounds or compensation. This means that companies will be less inclined to offer services or payment in exchange for the user rights to personal data. After all, consumers could have the information concerned removed at any time after having received said payments or service.

A better way of balancing the pros and cons of the right to erasure would be to include a compensation for the company involved if and when citizens one-sidedly decide to terminate the privacy agreement. In the case of online subscriptions this could mean that consumers pay a higher monthly subscription fee if they should decide that their personal data can no longer be used by the online company. In the example of telecommunications company AT&T, the agreement could offer the customer the option of returning to the more expensive subscription fee without data collection. In this way, people could simply reverse their decision, while companies would have more certainty about the sustainability of user rights.

[23] Article 17 of the proposed regulation on data protection ('the right to erasure') states that the person involved ('data subject') has the right to withdraw his consent to use his personal data as intended under (a) of Article 6(1). This last article states that personal data may be used for one or multiple specific purposes if the person involved has given their consent.

Policy option 2. Standard agreement without purpose limitation

Allow a standard agreement under which purpose limitation has been replaced by more general conditions of use, so that permission may be given for the reuse of data.

Purpose limitation means that privacy agreements between citizens and businesses always must specify the purpose for which the personal data will be used. Thus, it is not possible to enter into an agreement that only stipulates general conditions for the use of personal data. This has the advantage of clarity, for all parties involved, about the purpose for which data may be used. Citizens, businesses and supervisory bodies all know exactly what can and cannot be done with the data. Purpose limitation, thus, helps consumers to be aware of how and where their personal data will be used.[24] Furthermore, purpose limitation means that the supervision on the use of personal data is cheaper, because misuse is easier to determine. The disadvantage of purpose limitation is that reuse of personal data is very costly, as it requires that a new agreement is drawn up for each new purpose. In many cases, such a new privacy agreement represents a sizeable expenditure that involves delays as well as uncertainty about the response of the individuals involved. This, in turn, makes innovation based on the reuse of personal data unattractive.

The advantages and disadvantages of purpose limitation could be balanced more effectively by allowing a second standard agreement in which the intended use of the personal data is only indicated in general terms, in addition to the currently stipulated standard agreement. Citizens could then indicate the categories of use they would consent to (e.g. 'specific advertisements', 'customer service' and 'market research'). Parties could choose themselves whether to use the standard agreement with purpose limitation - and thus with more supervision - or the second type of agreement without purpose limitation but with greater flexibility. A more flexible agreement does give companies a greater responsibility of having to explain what they are doing with the data (Roosendaal, Van den Broek and Van Veenstra, 2014). An added advantage of having an agreement without purpose limitation for more sophisticated products is the fact that these agreements can be short and simple. This increases the chances of people reading and truly understanding these agreements, which in turn improves their ability to decide on whether to provide others with their personal data.

Policy option 3. More clearly describe the legitimate interest

For new applications, the supervisory body should be able to provide clarity about whether or not a legitimate interest may be claimed. This could for example be done by formulating clear, general principles that companies could use to assess the possibilities for themselves.

Not in all cases would companies be required to ask permission for the use of personal data. It is unnecessary for the general operations or everyday management of the organisation. These objectives are considered a 'legitimate interest' in the use of personal data. Companies must determine for themselves whether their interest in using the data outweighs the interest of the person involved. Although claims of legitimate interest are not limited to special occasions, companies cannot automatically claim such an interest.[25]

[24] Unless purpose limitation leads to more complex agreements – in those cases the reverse is more likely.
[25] Opinion 06/2014 of the collaboration framework of European privacy supervisory bodies (the 'Article 29 working group') on legitimate interest.

How companies should weigh these interests in situations that have not been described by the supervisory body, is unclear. By formulating general principles, the supervisory body will keep this uncertainty to a minimum. Such an open standard ('fair use') is already used in copyright. It leads to fewer transaction costs, fewer hold-up problems and creates more scope for innovation. Too much leeway leads to lower transaction costs, but also makes it more difficult for citizens to prevent that certain personal data are being collected. An open standard, therefore, is particularly suitable for basic personal data (e.g. name, address, telephone number, email address) and for situations in which personal data are more or less immediately anonymised, such as using Wi-Fi tracking when counting passers-by.

Policy option 4. Certification

Use certification to indicate the level of privacy that is related to a product.

Complex privacy agreements and moral hazard make it difficult for citizens to base their decisions on the privacy policy of companies. In addition to the already discussed options, supervisory bodies could also contribute to improved insight by applying certification. Supervisory bodies, currently, only publicise the way in which a company handles personal data when regulation is being violated. By applying certification labels, a supervisory body would thereby inform citizens of which companies are following regulation. In this way, market failures due to moral hazard could be combated, as the trust in companies with a certification label would be greater.

Certification labels are particularly beneficial for smaller companies and start-ups. For smaller companies, having a certification label is a substitute for having a positive reputation; it makes it easier to compete with larger companies. Certification labels, incidentally, are not the exclusive domain of the government, but may also and just as effectively be introduced by private parties.

Policy option 5. Privacy Enhancing Technologies

Create a public identification platform that is inter-operational with private Privacy Enhancing Technologies (PETs), and introduce a permit system for crucial PET services.

One of the responses to the increase in the use of personal data is the development of software that enables citizens to maintain a greater level of control over their personal data. These privacy-enhancing technologies (PETs), initially, were mostly intended to facilitate anonymous internet use, but more recent PETs focus on personal data management. Companies can apply PETs after they have collected personal data, thus reducing the risks of data leakage, but PETs may also be used to provide citizens with a larger degree of control over with whom they share their personal data. Examples of Dutch PETs are eID, a public service that enables personal online identification, and Qiy, a service that provides citizens with control over which of their personal data they share and with whom.

The advantage of PETs is that they reduce the chances of moral hazard, which also gives citizens a greater sense of security when they share their personal data. Companies, in addition, have more certainty about the correctness of data (Acquisti 2008). An added advantage is that PETs can greatly reduce the transaction costs of privacy agreements. The government may stimulate the use of PETs by facilitating electronic identification. Although private parties could also provide identification, the role of the government adds advantages of scale, the authoritative position of identity manager, standardisation, and the prevention of double identities. Thus, PETs offer the government the possibility of fulfilling their public tasks more efficiently.

Private PET services, at some point, may become essential for many types of transactions and in the management of sensitive personal data. In order to guarantee the reliability of such crucial PET services, a permit system could be put in place – similar to that of the financial sector.

Policy option 6. European supervisory body

A European supervisory body could be established for companies that operate on an international level, with national supervisory bodies such as the Dutch Data Protection Authority (CBP) focusing on domestic activities.

Supervision within Europe, currently, occurs on a national level, which also leads to twice the amount of work in cases of monitoring and sometimes sanctioning of multinationals. To avoid this double amount of work and to increase the level of safety for citizens and companies, the proposed regulation states that, in such international cases, the responsibility must be placed under one supervisory body. This is the so-called *one-stop shop*.

European collaboration could be more efficient than it is today. A central European supervisory body with authorisations comparable to those of the EU Directorate General for Competition would have two advantages. The first being that national supervisory bodies would not all need to have the technical and legal expertise to determine whether a company with sophisticated technology would be in violation.

A second advantage is that a European supervisory body would prevent free-rider behaviour in national supervisory bodies. As a national supervisory body could feel less urgency to reserve capacity for checking companies that do not focus on the domestic market. Moreover, a small supervisory body would rather leave the prosecution of large multinationals to larger

supervisory bodies. European supervision, thus, is likely to deliver more decisiveness than a collaboration of national supervisory bodies would.

Conclusion

The possibilities for the use of personal data in the economy have strongly increased over the past years. Citizens, consumers, entrepreneurs and employers have all benefited from this development. Things also go wrong on a regular basis, causing the privacy of citizens to be violated. Interests are great and it stands to reason that personal data use will intensify in the future. Effective privacy policy, therefore, is crucial to our prosperity. The diversity in preferences and fast technological developments mean that a market for transferable user rights to personal data should be the focus of privacy policy. This study discusses a number of policy options that would improve the functioning of this market.

References

Acquisti, A. and J. Grossklags, 2005, Privacy and Rationality in Individual Decision Making, *IEEE Security and Privacy*, vol. 3, nr. 1, pp. 26-33.

Acquisti, A., 2008, Identity Management, Privacy, and Price Discrimination, *IEEE Security and Privacy*, vol. 6, nr. 2, pp. 46-50.

Acquisti, A., L. John and G. Loewenstein, 2009, What is privacy worth, Twenty first workshop on information systems and economics (WISE), pp. 14-15.

Athey, S., 2014, Information, Privacy, and the Internet: An Economic Perspective, CPB Lecture 2014.

Berg, G.J., 2006, Revolutionary Effects of New Information Technologies, *The Economic Journal*, vol. 116, nr. 509, pp. F10-F28.

Campbell, J., A. Goldfarb and C. Tucker, 2014, Privacy regulation and market structure, *Journal of Economics and Management Strategy*.

Kelley, P.G., L. Cesca, J. Bresee and L.F. Cranor, 2010, Standardizing privacy notices: an online study of the nutrition label approach, Proceedings of the SIGCHI Conference on Human factors in Computing Systems, pp. 1573-1582.

Mcdonald, A.M., R.W. Reeder, P.G. Kelley and L.F. Cranor, 2009, A comparative study of online privacy policies and formats, Privacy enhancing technologies, pp. 37-55, Springer.

Roosendaal, A., Tijs van den Broek and Anne Fleur van Veenstra, 2014, Vertrouwen in big data toepassingen: accountability en eigenaarschap als waarborgen voor privacy, *Privacy en Informatie*, vol. 2014, nr. 3.

Turow, J., Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, 2009, Americans reject tailored advertising and three activities that enable it, Annenberg School for Communication Working Paper.

Yandle, T. and C.M. Dewees, 2008, Consolidation in an individual transferable quota regime: lessons from New Zealand, 1986–1999, *Environmental management*, vol. 41, nr. 6, pp. 915-928.

Publisher:

CPB Netherlands Bureau for Economic Policy Analysis
P.O. box 80510 | 2508 GM The Hague
T +31 70 3383 380

June 2014 | ISBN 978-90-5833-646-0