Hans de Bruijn and Bram Klievink

Holy Privacy[1]

Not too long ago, many internet users shrugged off the issue of data privacy. 'Nothing to hide', was the mantra. Yes, we hand over vast volumes of data points – but so do billions of other users. Data ends up somewhere on the bottom of the data ocean, one might think – and every day a new layer of a few quintillion data points is laid on top of the existing layers. The numbers are so staggering that they fuel the idea that our data will never be recovered, by anyone.
That is a dangerously simple train of thought. Data privacy is a big problem – so big that, actually, the word 'privacy' is misleading, is too much of a remnant of days gone by. Once we traveled on horseback. Nowadays, we travel with an intercontinental flight. It would be strange if we were still using the word 'horse' to describe an airplane, because that it still is a means of transportation – but something to this effect happens with the concept of 'privacy'. The nature of privacy violations has changed fundamentally, and a current privacy violation is something quite different from what it was in the pre-Web world. Yet we still use that word 'privacy'.

About this essay

Privacy has developed into a much more complex, multi-layered concept. In this essay, we begin with peeling back the different layers of the concept of privacy. The conclusion will be that 'privacy' - we will have to stick to this concept - and privacy protection are major problems. We may expect governments are fully committed to protecting the sharing and use of data - which they are indeed, and, fortunately, there is much more focus on privacy in public debate than before. However, in our ever digitizing society, data is crucial. Data can contribute to innovation – to more safety, better care, better education. And we may also expect our governments to do their utmost to promote safety, proper care and proper education. To a certain extent, we feel this element is lacking in the public debate.

Privacy as a multi-layered concept

In the pre-Web world, the concept of privacy is well summarized in the British proverb 'My home is my castle'. We live behind a wall that guarantees privacy. As the resident of the castle, we decide which information is to leave the castle. Privacy means that (1) something will remain a secret, and that (2) we are in control.

---

[1] Translated from Dutch and printed here with permission from the authors.
Please refer to and cite the original newspaper article (in Dutch): De Bruijn, H. & Klievink, B. *Die heilige privacy*. Trouw, 4 December 2021: https://www.trouw.nl/cultuur-media/geef-eens-wat-privacy-op-en-maak-de-wereld-zo-een-beetje-mooier~b5a0ba90/

Privacy in our data-driven world has become a concept with at least four layers – in addition to the proverbial 'my home is my castle'.[2]

The earthquake and the dormant volcano

One. In the past, private information ended up in a tabloid or in the newspapers – and, as the old saying goes 'today's news is tomorrow's fish-and-chip paper'. Now, private information ends up on the internet and stays accessible to everyone, forever. The appropriate metaphor is the earthquake with shocks and aftershocks. Whoever becomes the victim of revenge porn, will feel this as a tremendous shock. But that's not all. Forevermore, the information will roam the internet. To resurface at the most impossible moments – like the aftershocks of an earthquake.
Another metaphor is the one of the dormant volcano: information that currently seems innocent, may prove to be anything but that at a later stage. The well-known example is 'sharenting' – parents who share stories about, and images of, their children online. This may be cute now, but when the kids grow up, they may feel this as a flagrant violation of their privacy. The dormant volcano erupts.

Profiling

Two. Data we hand over is also used to profile us. There is much research with the message that it takes a relatively limited dataset to create a person's profile – about someone's mental state, political preference, purchasing behaviour, emotions, secret longings. Think of the Cambridge Analytica scandal of a few years ago: Facebook likes were used to determine a person's character traits. But, it really isn't solely Facebook data that can be used to profile. Data about search behaviour, about the use of smartphones, data on Instagram accounts: these can all being used to profile people.

Capturing

Three. When we are being profiled, we can receive better information. Our purchasing- or search behaviour shows that we are interested in green parakeets, so we will be offered information about green parakeets. This is mostly harmless, but informing us may change into manipulating us. Thanks to profiling, criminals can refine their spoofing strategy by constructing better and more convincing fake identities. Politicians can micro-target us, with messages we are susceptible to – and which may sometimes be downright nonsense. Governments can place us in a box with their algorithms and subsequently their enforcers can go after us - or not.
And then, there are the reinforcement algorithms of the tech-giants, who continuously feed us information that is in line with our profile and our preconceptions – and which confirms us in being right in a continual fashion. You

[2] These sections based on Hans de Bruijn (2021) *The Governance of Privacy Privacy as Process: The Need for Resilient Governance*, Amsterdam: Amsterdam University Press

are of the opinion that all bankers are fraudsters – and, subsequently, you are being bombarded with information that tells you all bankers are fraudsters. We become a prisoner of our own convictions.

The soul of a nation

Four. When all this takes place at a grand scale – this does not only impact the individual, but also society as a whole. Manipulation and the continual confirmation of our preconceptions being right, may create a toxic atmosphere in a society and boost societal antagonism. This is particularly true for a society already divided – think of present day America, or of the tensions between the vaccinated and unvaccinated during the covid crisis.

The radical transformation of privacy

This multi-layered character makes privacy and privacy breaches fundamentally different from the pre-Web concept of privacy. Then, it revolved around private information leaving the castle. A movement from the inside out. Now, it entails a movement from the outside in: you as the resident of the castle, are being profiled by parties outside the castle, and subsequently manipulated. Then, the consequences of a
privacy violation predominantly impacted the individual. Now, it concerns society as a whole.

Source: Hans de Bruijn (2021), The Governance of Privacy, Amsterdam: Amsterdam University Press

Regulations

Meanwhile, legislation and regulations are being issued in order to rein in the gathering and use of data – with Europe as the frontrunner. The position of privacy watchdogs is being strengthened – although there still lies a road

ahead. The political aversion to the data-robbing tech-giants is growing. Organisations that do not properly protect this personal data, may face sky-high fines. Employees unnecessarily looked into the files of a famous person? A fine of several hundred thousands ensues. British Airways does a poor job protecting customer data? A penalty of twenty million pounds - the British watchdog

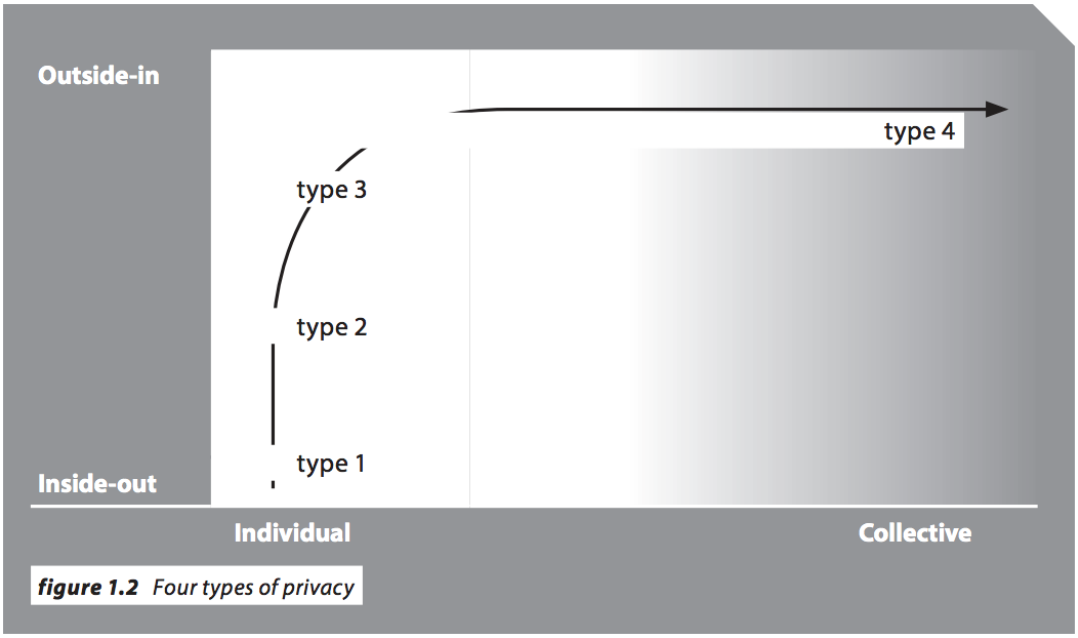

figure 1.2 *Four types of privacy*

formulates it beautifully: 'People entrusted their personal details to BA and BA failed to take adequate measures to keep those details secure (…) When organisations take poor decisions around people's personal data, that can have a real impact on people's lives.'[3]

Data brings innovation

So far so good. Yet, there also exists another story, one that is given less attention in the public debate on data privacy. Data in an era of digitization is sometimes compared to electricity: electricity has led to a tremendous societal dynamic and innovations. No-one has been able to predict or imagine this. This may also happen to data in an era of digitization: we know that this will lead to many more innovations, we just aren't aware of which ones.
In addition to this, data and digitization do not just imply better service here and there, they also entail an infrastructure – the future backbone of society, which can be compared to railroad tracks, roads, an electricity grid. We all know that a modern infrastructure is crucial to public prosperity. And then, the question is: what does data protection mean in terms of digital innovation? Take Europe: it has a well-constructed legal system of data protection – and more regulation is underway. How does data privacy relate to digital innovation? That is a

[3] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

question one can answer in at least two ways, which we summarize under the labels ‘direction’ and ‘space’.

Privacy protection is conducive to innovation

The first answer is, that privacy protection provides direction to innovations. One determines rules for data protection and, as such, delineates the space for innovation. This may work: there are many domains for which government determines rules, without negatively impacting innovation. A well-conceived system of regulation, such as the European legislation for data protection, provides a predictable environment for companies - and predictability and stability are important conditions for change and innovation. There are many more arguments in favor of the position that regulation is conducive to innovation. Europe is an economic power block, so Europe can make demands on internationally operating companies, that operate within the EU market. There is something that is called the Brussels-effect: companies abide by the strict European rules, as they thereby comply with all regulations worldwide. Also, more regulation of privacy means more consumer attention to privacy – and so it becomes appealing to companies to present privacy-friendly products and services. Users may choose from various browsers, chat services, search-engines, devices – that may distinguish themselves, among other, through the privacy protection they offer.
Rather than being at the expense of innovation, data protection provides direction to innovations.

Privacy versus innovation: a constantly changing value trade-off

There is however a second answer. Data can be used for services we value highly: more safety, better care, better education – and much much more.
So, we always have to strike a balance between the use of data and innovation. Sometimes, these are difficult trade-offs: do we want more privacy or more safety, or better care? Besides, our convictions about this particular balance may change. A pandemic, for example, has such an impact on society, that the preferred trade-off between privacy and care may shift. During the corona pandemic, the United Kingdom created a list of vulnerable patients, in order to provide additional information to them. This data was provided by hospitals and physicians. The UK’s Information Commissioner's Office: 'The ICO is a reasonable and pragmatic regulator, (…), we will take into account the compelling public interest in the current health emergency.’[4]

There is not only the need for a trade-off, but the question is also when we will make this trade-off between privacy and other values? There is a popular answer to his question: as early as possible, upfront, upstream in the innovation process - the concept of ‘privacy by design’ is based upon this idea. However, in

[4] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/

the early phases of an innovation process it will often be unclear what the ultimate innovation will be.[5] It is not always clear what the early stages of an innovation process are - innovation is not always a linear process with a beginning and an end. More importantly, the innovation might change our opinions on the tradeoff between privacy and other values. Thanks to innovative devices, data help us to become more fit, maybe in such a way that the balance between privacy and health is tilted towards health.
Hence, the trade-off between privacy and these innovations cannot always be made at the start of an innovation process. Innovation is by nature experimenting, trying out, and learning. Only once this innovation has occurred, we can come to a well-informed trade-off between data use and the value of the innovation. So, you have to provide space to innovation, refrain from obstructing it too early.

An example

Direction or space – let's use facial recognition as an example. Facial recognition is a highly sensitive subject in terms of privacy – and so, one might opt for clearly determined rules for its use. As such, regulation provides direction to the innovation process. But of course this creates the risk that certain innovations are not given the chance to develop.
We can also choose the strategy of offering space to this technology. Various unpredictable innovations may occur. These will influence our opinion on privacy versus safety. Suppose that systems of facial recognition contribute to solving violent crimes in nightlife areas. This may mean, that the societal tolerance for unsolved violent crimes will be lessened significantly – the idea that someone is being molested in the street and that, subsequently, the perpetrator highly likely isn't punished, is increasingly unacceptable to us.
This change of view may be of great impact on our normative appreciation of facial recognition and on the trade-off between privacy and more safety – which may be at the cost of privacy. In the concept of 'direction' our moral views determine the innovation. In the concept of 'space', innovations may influence our moral views.
Of course, the concept of 'space' may also entail that we learn that facial recognition does not bring us anything good, and is not worth the price of privacy. We might be faced with a serious risk then: we give space to the innovation, but we will not always succeed in undoing innovations we do not like.

A thought experiment

Direction or space: it is a difficult dilemma. Do we impose restrictions on innovation processes, upstream or downstream? When we impose restrictions

[5] Some public value gains through data-driven innovation may never be realised if this needs to be settled early in the process, see: Klievink, B., van der Voort, H., & Veeneman, W. (2018). Creating value through data collaboratives: Balancing innovation and control. *Information Polity*, *23*(4), 379–397. https://doi.org/10.3233/IP-180070

upstream, we run the risk that certain innovations do not stand a chance? If we do this downstream, you want to restrict afterwards – will we still succeed in blockading innovations? Or is the innovation unstoppable, in the final phase of the innovation process?
In order to indicate the difficulty of the dilemma, a thought experiment.
Take two economic power blocks. Block A highly values privacy protection and strongly commits to it. Block B highly values innovation – and pursues 'data-friendly' policies. Since block B has less restrictions, all kinds of innovations may occur. When these prove to lead to too much infringement on privacy, the citizens of block A are happy – they always leaned towards privacy.

Now, suppose that within block B, more safety occurs in the streets, and better health care, more tailor-made education. And suppose the moral view develops that this improvement of quality justifies less emphasis on the interest of privacy. In the meantime, privacy in block A is well-protected, but as a consequence there are less innovations in the police force, in healthcare and in education. The question rises how long the strict privacy policy of block A will hold – when citizens of A see that the public service in block B is of a much higher level. This may lead to a dramatic conclusion for block A. It learns what is possible in terms of better service in B, and wants that too. But meanwhile, block A has a technological disadvantage to block B – while block B's new technologies find their way to block A, unhindered by competition from a more privacy friendly alternative.
Again, this is a thought experiment and reality is, of course, much more complicated. For us, it is important that the issue of innovation also gets its place in the debate about data privacy.

Tech-cowboys, good guys and bad guys

The rapid growth of tech-giants such as Facebook often invokes the image of the Wild West. Young tech entrepreneurs such as Facebook's Mark Zuckerberg possessed new technologies, and developed new data-driven services – which grew exponentially in no-time. For these new technologies and services, hardly any legislation was in place. So these entrepreneurs could behave like cowboys – they robbed our data and expanded their domain, not being hindered by anything or anyone. We think that Facebook services are free – but we pay with our data and, as such, with our privacy.
The tech-cowboys have caused tremendous damage. But meanwhile, the sheriff is in town – rules are being issued, and the sheriff fights for law and order.
Privacy protection revolves around at least two balancing acts. First, the one between the important interest of privacy and the important interest of innovation. And then there is the question whether governments should provide direction – or provide space. The debate on privacy can easily end up in a good guy - bad guy frame: those who protect privacy versus those who breach privacy. The dilemmas show that this is really too simple. If we do not realise this,

the privacy debate will remain a Western, with the good guys chasing the bad guys.