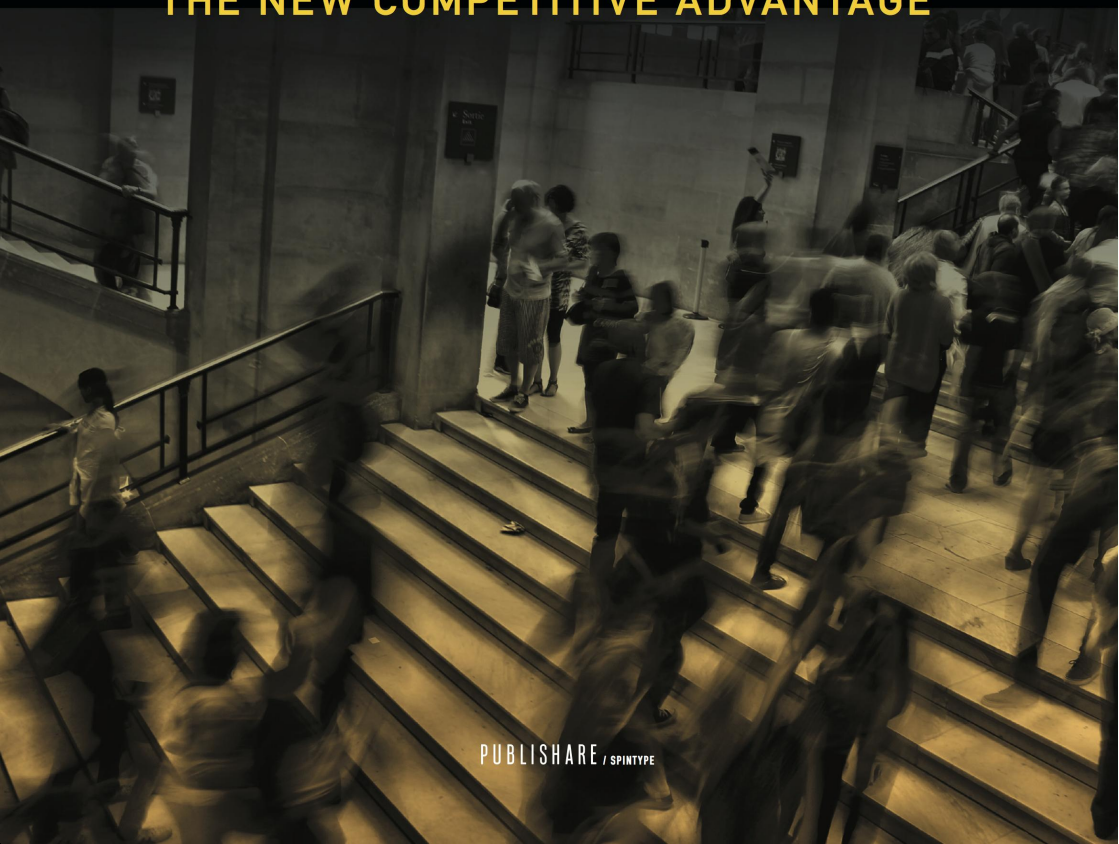
Gry Hasselbalch & Pernille Tranberg

DATA ETHICS

THE NEW COMPETITIVE ADVANTAGE



PUBLISHARE / SPINTYPE

DATA ETHICS - THE NEW COMPETITIVE ADVANTAGE

1. edition, 2016

Authors: Gry Hasselbalch & Pernille Tranberg
Graphics: Publishare ApS / Spintype.com
Cover: Per-Ole Lind
Photos: Unsplash.com
Editor: Francesco Lapenta
English language revision: Katherine Kirby

Print: AKA PRINT A/S
ISBN print: 978-87-7192-017-8
ISBN pdf: 978-87-7192-018-5
ISBN epub: 978-87-7192-019-2

Supported by Internet Society

TABLE OF CONTENTS

Data ethics is potential, new market growth, a sustainable strategy and the foundation of creative, innovative business processes.

INTRODUCTION

THE DATA ETHICAL PARADIGM SHIFT

We are living in an era defined and shaped by data. Data makes the world go round. It is politics, it is culture, it is everyday life and it is business. Our data-flooded era is one of technological progress, with tides rising at a never seen before pace. Roles, rights and responsibilities are reorganised and new ethical questions posed. Data ethics must and will be a new compass to guide us.

Two decades ago, environmental reporting was something quite new, and many companies did not take being 'green' very seriously. There was growing concern among good-intentioned citizens, but many didn't know how to act on it. Today, those same worried individuals can sort their garbage, eat organic foods, take warm, solar-powered showers and drive electric cars. Companies also take the environment seriously. Not only because those with a direct effect on the environment are required to report to the authorities, but because green business practices are sound business practices.

Being eco-friendly has become an investor demand, a legal requirement, a thriving market and a clear competitive advantage. Data ethics will develop similarly – just much faster.

Data leaks, hacks, surveillance scandals and, especially, social media users' 'digital hangovers' (Chap. 1) have kick-started a movement. Individuals and consumers aren't simply concerned about a lack of control over their personal data (their privacy), they're starting to take action on it and react with protests, ad blockers and encrypted services (Chap. 3). In Europe, a new data protection regulatory framework which encourages the development of a privacy by default infrastructure has been implemented. Across the globe, we're seeing a data ethics paradigm shift take the shape of a social movement, a cultural shift and a technological and legal development that increasingly places humans at the centre.

Businesses are starting to feel this shift. Not as an 'either/or', either we use data or we don't, but rather they're gaining awareness about data from an ethical perspective, gradually moving away from an overbearing focus on big data (Chap. 5) and embracing sustainable data use. Visionary companies are already positioning themselves within this movement (Chap. 4) and investments in companies with data ethics are on the rise (Chap. 8). We're seeing an increasing number of businesses take the development of privacy technology as a direct point of departure (Chap. 6), along with the value of individual data control (Chap.12).

WHAT IS DATA ETHICS?

Ethical companies in today's big data era are doing more than just complying with data protection legislation. They also follow the spirit and vision of the legislation by listening closely to their customers. They're implementing credible and clear transparency policies for data management. They're only processing necessary data and developing privacy-aware corporate cultures and organisational structures. Some are developing products and services using Privacy by Design (Chap. 7).

A data-ethical company sustains ethical values relating to data, asking: Is this something I myself would accept as a consumer? Is this something I want my children to grow up with?

A company's degree of 'data ethics awareness' is not only crucial for survival in a market where consumers progressively set the bar, it's also necessary for society as a whole. It plays a similar role as a company's environmental conscience – essential for company survival, but also for the planet's welfare.

Yet there isn't a one-size-fits-all solution, perfect for every ethical dilemma. We're in an age of experimentation where laws, technology and, perhaps most importantly, our limits as individuals are tested and negotiated on a daily basis.

THE FOURTH INDUSTRIAL REVOLUTION

In the wake of today's rapid technological development, human and ethical dilemmas emerge (Chap. 11). Data is transforming society – some call it the Fourth Industrial Revolution. The first industrial revolution was based on water and steam, the next on electricity, and the third on information and digitalisation. In the fourth, the boundaries between the physical-biological and digital worlds are being eliminated – fuelled by data.

Data, personal data included, can have many positive uses and outcomes, but there are also many risks in a data-driven business process (Chap. 2). Gartner Inc. has predicted that by 2018, 50% of business ethics violations will occur due to improper use of big data.

GLOBAL STANDARDS FOR DATA ETHICS

Data is an asset, but it's also a risk. Today, the most prominent perils are data exhaust and unsustainable data practices, and a process to negotiate global standards, roles, rights and responsibilities to handle such risks has been initiated. This also means that tensions and clashes between laws and cultural values are amplified (Chap. 10).

Throughout history, societies have always somehow managed to mitigate man-made risks produced by different periods of industrialisation (e.g. pollution, atomic weapons and health hazards in food production) through new regulations, global standards, formal verification systems which consumers trust, and slow but steady cultural adaptation – including new levels of awareness, education, literacy and ethics. Industry has had to adapt to these requirements not only with targeted risk assessment and management, but by innovating and evolving in new ways. It will have to do the same in a data-saturated environment, with data ethics as a guide.

FAIRER MARKET CONDITIONS

There are several worrisome legislative circumstances worldwide that support indiscriminate mass surveillance of residents, back doors in technologies and greater secrecy shrouding intelligence services' monitoring activities. But there are also promising efforts which indicate a certain level of political understanding in relation to the privacy challenges inherent to the current digital infrastructure, as well as data's status as a new type of power. Although it's clear that many interests have had a say in the new EU data protection regulation (Chap. 9), it's still rather well thought out and attempts to look ahead to the technological evolution of the future. If enforced equally for both EU and non-EU companies and supported by anti-trust and consumer protection laws, there's a good chance that competition in the lucrative European market will be fairer than we have seen it the previous decade.

Regulation may point the way forward, but laws alone do not create fair market conditions or ethical business practices. Currently, companies can 'legally' use data in far more ways than what is in the individuals' best interest. Therefore, individuals must also take responsibility over their own data. It's a three-way hub of responsibility between regulators, individuals and businesses.

PRIVACY FOR THE ELITE

The societal repercussions of unregulated, ethics-free data practices are numerous, but the damage done to individual privacy is at its core. In a properly functioning democracy, those in power – government, industry and organisations -– are open and transparent about how they exercise their power. But one cannot expect transparency from individuals, as the more transparent people are, the more vulnerable they become (Chap. 13).

While laws, business practices, common international standards and cultural frameworks are being negotiated, privacy will be for the elite.

The highly educated, well-off, well-known and powerful will feel the need and will be able to pay for their privacy and control over their data. But as with the environment, a more formal framework for data ethics business practices will develop. A market for privacy tech and data ethics products will evolve, prices will go down and more people will gain access to them.

ABOUT THIS BOOK

This book is an analysis of trends through which we map a new field by looking at a few constructive solutions. This also means we address the forces at play in general, that is: the societal power structures, interests and relationships underpinning the field. It's fundamentally

important to us to make the invisible visible and, as such, provide the right tools to build something new: data-ethical services, businesses and products based on a paradigm shift in the way we approach digital data.

We hope to inspire companies large and small, as well as a wider audience of professionals who are not necessarily working in technology and data, but who wish to get a head start in the data ethics field. We have included more than 50 examples of practises that, in one way or another, are ethical when it comes to data. The examples were collected through interviews, credible media reports and website statements. We are not endorsing the companies, we do not compare their approaches, nor do we analyse all their practices. We are solely using them as case studies to provide the reader with inspiration for further exploration of the topic.

Most of the companies mentioned are still in a beta phase in the data ethics field, and not one has yet found the optimal solution. Every beginning takes time, just as it did with the products and companies that arose from the first inkling of environmental awareness.

Gry Hasselbalch & Pernille Tranberg, October 2016

In today's most common digital business model, consumers pay for 'free' products with their personal data.

CHAPTER 1

DIGITAL HANGOVERS

The year is 2006. *Time* magazine has awarded 'you' Person of the Year. *You* the active, productive web 2.0 user. *You* who use social media to share information, pictures and stories about yourself. *You* are hereby placed in the same category as Gandhi, Obama, Mark Zuckerberg and even the Earth: people and planets that throughout the years all have been named *Time*'s Person of the Year.

The 2006 award was recognition of online media's progress with the user at the centre. Social media, web 2.0 and active user centric services formed the most important trend in digital business development. Previously by invitation only, Facebook opened its social network up to everyone that year and Twitter launched as the first 'micro-blogging' site.

Traditional news media also jumped on the bandwagon. That same year, CNN became one of the first news media outlets to expand its services with *iReport*, inviting users to submit their own videos and photos from events around the world. Even savvy politicians found their very own channel in social media. In 2008 a relatively unknown man, at least from a global perspective, was elected president of the United States of America, partly based on a massive social media campaign and the use of data on the American electorate.

All of this happened because everyday people greeted social media with overwhelming enthusiasm. At first, it was trendsetters and young

people to use social media as part of their unique online identity. With photos, text and music they created online networks where they could coordinate social events with friends; they built a 'completely private' space sheltered from the prying eyes of concerned adults. It didn't take long before mum, dad, grandma and grandpa jumped on the web 2.0. train and began to 'poke' each other.

And what a party it was. The public media debate inspired somersaults of excitement for all the new opportunities: weblogs and moblogs, Youtube, Second Life, Myspace, Twitter, and something called Jaikuu. *You* were in the midst of sharing your life online. 'See my delicious menus, see my travels, see my baby. See me. Hear my opinion about shopping malls, lobsters and vitamins and politicians and skyscrapers and cars with three wheels! See, here I am at a party, so happy, loved by others...hey, that picture...can we delete that?'

OOPS, WE'RE ALL PUBLIC

It didn't take long before those same everyday people began to feel a bit of a digital web 2.0 hangover. Many had made a misplaced comment in the wrong context or posted pictures on social media that didn't quite fit their image. Parents began to check on their teens online and intervene in their social lives. We were misunderstood, some of us became enemies and some were even fired from our jobs.

Organisations, the media and politicians quickly shifted their focus towards the potential consequences of ordinary people suddenly becoming public figures with their lives freely available on social media. The original emphasis on Internet security evolved into a focus on responsible and ethical social media use. 'You are what you upload' declared one slogan. Then there was the danger of adult paedophiles, lurking in the dark corners of open social networking services. 'Never share your phone number', 'Don't talk to strangers online', children were taught. Another catchphrase reminded, 'You're the one who sets the limits', a mantra that, suddenly, web 2.0 users desperately needed to hear repeated; they were beginning to feel they had lost control.

Campaigns, safe chat rules, social media codes of conduct, guidelines and recommendations were all implemented. Everyone joined in, even the biggest social networking services themselves. Users were invited to adjust their 'privacy settings' and divide their networked friends into groups. One for colleagues. One for the family. One for friends. Public profiles were so last year. Facebook was seen as the most original trendsetter because they had private profiles, only accessible within the network, unlike its predecessor Myspace where your profile was viewable by anyone who stumbled upon it. The public debate began to slowly tune in to the more problematic aspects of web 2.0. We all had a web 2.0 hangover and we needed a cure. Social media services that didn't react fast enough lost the battle, or perhaps they just became necessary sacrifices in the first wave of public data ethics. Users lost confidence in the earlier social media sites and jumped on the bandwagon to ones which they thought they could trust (especially when their children were involved) and which offered them anything even slightly resembling control of their digital identities. We can all think of at least one open social media network that we used to have a profile on. (Did you remember to delete it?)

PERSONAL DATA BECOMES COMMERCIALLY VALUABLE

Parallel to the web 2.0 rush, two other trends were moving briskly along. The first trend was the foundation of Internet businesses after the first dot-com bubble. In the 1990s Ethan Zuckerman, the current head of the MIT Center for Civic Action, was working in one of the first Internet-based companies, Tripod.com. He offers insight into how an online business model based on targeted marketing came into being. Tripod.com had experimented with many different business models: subscriptions, shared user payments and even selling t-shirts. In the end, they landed on targeted marketing; meaning, as critics later pointed out, when something is free (or very cheap), you are the product. Under this business model, Tripod.com analysed users' personal web pages so they could target advertising to them. They chose

this route because it was the easiest one to sell to investors. As Zuckerman put it, the Internet was seen as "Christmas Eve for advertising and marketing people".[1]

The second trend was a society- and business-driven focus on data collection and storage, what is also referred to as big data. Knowledge, information and data have always been an important aspect of a company's business. But storing and analysing data before the age of the Internet required extensive resources. With the development of databases and analytical software, the cost of collecting and using data was significantly reduced. The Internet, web 2.0 and cloud computing, which made it cheaper to store data than delete it, created an additional foundation for what we now normally refer to as the data-driven business model, one founded on droves of data - big data.

BIG DATA RELIGION

Consumer tech giants such as Facebook, Google/Youtube, Amazon, Twitter, and Tencent have built their business models on the collection of data. Normally, they're described as social networking services and trading platforms, but they're also big data companies. Along with the more invisible data brokers that sell access to and trade data, they hold the world's largest troves of personal data with a growing range of applications. Data is at the core of their business models and processes, and these companies are assessed on the amounts of data they hold, their ability to put it to use and their capacity to innovate with it. The more data, the better. As Professor Viktor Mayer-Schönberger and the economist Kenneth Cukier posit in their book *Big Data* [2], the value of big data lies not only in the way we use data here and now, but also in the potential, future use of the volumes of data collected.The driving force for this type of big data business is the idea that large amounts of

1. Advertising is the Internet's Original Sin, The Atlantic, 2014.

2. Big Data: A Revolution That Will Transform How We Live, Work, and Think, Viktor Mayer-Schonberger, Kenneth Cukier, John Murray Publishers, 2013.

data equals great potential. It's an idea that can be translated into a type of big data religion or philosophy, as journalist Jacob Silverman argued in his criticism of the social media business model.[3] This corporate ideal is based on an almost metaphysical belief in raw data, where all data is seen as potentially useful and a potential road to success. In combination, the Internet, web 2.0 and big data business ideals evolved into a business model built on trackable aggregations of personal data. The resulting online infrastructure has a default setting which collects and stores data; it's a space where individuals are public and trackable by default.

The idea of big data has been a radically influential trend, not only in business development but also in science, governance, international development and surveillance. Methods based on the analysis of big data are being developed to manage natural disasters (by governments and humanitarian organisations), to trace the evolution of viruses across continents (by companies tracking the use of search terms), to follow electorates (by presidential candidates), and to predict individuals' future health situations (by insurance companies), potential criminal acts (by law enforcement), and the formation of romantic relationships (by social media scientists). Intelligence services are acquiring increasing access to archives of big data on citizens whom they want to keep an eye on.

Big data is just as great of a societal force of change as industrialisation was, and just as the industrialisation of societies brought about potential and growth, there are also many negative consequences.

The same can and will be said about the datafication of societies. We're slowly beginning to generate data through the things that surround us in our everyday lives. In 1984, science fiction author William Gibson described a virtual network, a cyberspace, he called it,

3. Terms of Service and the Price of Constant Connection, Harper Collins, 2015.

which citizens could connect, disconnect or be disconnected from.[4] In the 21st century it is increasingly difficult to fully log out of the online space. The concept of the Internet of Things (IoT) is used to describe the increasing number of objects in our environment which are connected to the Internet and which process data about us and our surroundings locally or in the cloud while we're at home or out and about. Smart cities, smart TVs, refrigerators, lamps, stereos, bracelets, watches and so on. Gartner Inc. has estimated that the Internet of Things in 2016 includes about 6 billion Internet connected objects and predicts that this number will increase to 20 billion in 2020.[5]

SURVEILLANCE REVELATIONS

Although big data already played a role in most institutional and industrial sectors in the years following the initial web 2.0 wave, it was a trend that few ordinary people cared about. More than anything else, the things that directly affected our personal lives and families were what created reactions. In other words, the immediate social challenges of being a everyday human, in public – when your boss followed your profile, when children exposed themselves online, when friends posted embarrassing pictures to a shared network. Users had their personalised web to worry about, while businesses had their targeted web to develop.

The digital hangovers which reflect an awareness of our data's secret life in a big data society are relatively new. They are the aftershocks of a series of events that illustrate specific risks associated with the storage of larger amounts of private data in the public global network. Most significantly, the episode with the most ramifications in the public sphere was whistle-blower Edward Snowden's 2013 revelations about the US National Security Agency's (NSA) big data surveillance

4. Neuromancer, The Berkley Publishing Group, 1984.

5. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Gartner News Room, 2015.

methods. As early as 2005, with the book No Place to Hide, *Washington Post* reporter Robert O' Harrow had described, in detail, the dangers of the growing commercial collection of private citizens' data, combined with US intelligence services' increased focus on big data monitoring methods after the attacks on the World Trade Center in 2001. The first documents that Snowden revealed showed how the NSA collected hundreds of millions of text messages, email addresses, contact information and locations of citizens worldwide, every day. The documents also describe the so called PRISM programme under which, since 2007, the NSA collected data on foreign citizens via nine major US Internet companies, including the biggest social media companies. This disclosure about mass surveillance also proved to be a significant new angle on the framework for transferring data between Europe and the US and, as follows, the economic cooperation between the two.

It began to dawn on people that web 2.0 was not only big data, it was also big brother. In the months after Snowden's revelations, users of traditional privacy protection digital services mushroomed. Anonymous search engine DuckDuckGo's users rose by 50% in 2013, encryption tools of Silent Circle grew by 400% in weekly sales, while the encrypted cloud service Spider Oak's footfall increased 150%. The negative consequences of big data had become painfully obvious.

> **SpiderOak.** With SpiderOak, you can store data, collaborate with others and backup data. The service is based on the zero-knowledge principle. This means that SpiderOak knows nothing about the encrypted data, which is not decrypted until you use a password on your own computer. The customer therefore has full and genuine control over his or her own data. It's not just end-to-end encryption, which can leave behind information such as so-called metadata. It's zero knowledge, according to the company.[6]

6. Products with Principle, Spideroak.com, 2016.

There are as many good ways to use data as there are ways to create data exhaust and contamination.

CHAPTER 2

THE DATA DRIVEN BUSINESS MODEL

Google's search algorithm and Facebook's news algorithm are as guarded and coveted today as the recipe for Coca-Cola was in the 20th century. Such trade secrets are precious to companies in an online market which has become one of the present era's most financially lucrative spaces – especially for the fastest innovators and implementers, and not least those who understand how to scale globally. And for most large companies betting on the online market, data is the currency, means of payment, and foundation of their business models.

The first digital cash cow was the banner-ad. It was the first device which online news outlets used to generate payment for the content they published. With banner ads, sites could promise advertisers access to 'people North of London'; it was a way to reach a specific, targeted group of customers within a geographic area. Google, which did not produce significant income for the first seven years, began to capitalise on its search engine to then generate large parts of its revenue from banner ads. They could go even further and match those same 'people north of London' with their interests according to their search history, which Google stored and categorised. For years, Google and numerous other companies capitalised greatly on the search term advertising model (Google Adwords). Yet a new competitive model soon entered the playing field: an online social network which not only correlated demographics and interests but also people's real life identi-

ties and networks, precisely because users had to sign in with their real name in order to use the service. Although it didn't make a profit the first five years of its existence either, Facebook could go further than Google and connect the dots of 'men who drink red wine are owners of a caravan, heterosexual and single' for advertisers. Today, both Google and Facebook are among the most lucrative online companies on the planet.

The main tool to gather user information, cookies, has been refined over the years, and Google and Facebook have taken the lion's share of the advertising revenues based on cookies. While traditional news media are left to fight over the digital giants' leftovers, other, more quickly evolving companies are inventing new ways to harvest personal data to build detailed individual profiles. Yet at the same time, cookies are becoming an endangered technological dinosaur. They're losing steam as people are beginning to effectively block them both with ad and cookie blockers. More recent tracking methods are, for example, device fingerprinting, where you can precisely identify and track user behaviour through knowledge about the devices and applications they use, the size of their device's screen, time zone, fonts, etc. At the same time, information such as location and other relevant personal data is mined from mobile apps and wearables measuring one's health. Not to mention the upcoming data harvesting embedded in IoT (the Internet of Things), a business area in which the largest data companies have already taken root.

DATA AS PAYMENT

Many consumer tech and social media giants have built their business models on personal data. They may be search engines, social media, digital trading platforms, streaming services and health trackers. But they are, more than anything else, big data companies that generate profit on personal data. Although not necessarily trading data directly, their currency is similar to the more hidden (and often even richer) data brokers and data analytics firms. Data brokers such as Acxiom,

Datalogix and Experian trade individual data profiles while data analytics firms such as Palantir crunch data for the US government in the hunt for terrorists and large-scale fraudsters. In combination, these data giants have some of the largest archives of personal information on citizens all over the world.

Many of the consumer-directed companies have something in common: their services are either very cheap or 'free'. You simply pay an invisible price with your data, by now the web's preferred payment method. Modern-day customers have grown accustomed to not spending real money for digital products and services. They pay with data. Consequently, the digital companies of the future will find it even harder to profit unless they too offer their services for free.

The free model of payment even applies to businesses, which may opt to use the free version of Google Analytics. They pay, however, with customer data – in other words, their company's control over customer data.

GOOD DATA

Personal data is, at its essence, people, but data has also been defined as today's raw material, modern day gold or oil. Almost all major consulting firms have at one point used these terms to describe data's role in the current business economy. Many governments are betting that their countries' economies will evolve and grow based on data. Looking further down the road, this strategy is not as problematic as it sounds from a privacy advocate's point of view, because the most profitable types of data are not those connected to individuals. As McKinsey reported in '*The Internet of Things: Mapping The Value Beyond the Hype*' (2015)[7], the biggest growth potential lies in data which is not personal,

7. James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon, McKinsey Global Institute, 2015.

such as that relating to weather, traffic and products, which can streamline production, logistics, distribution and service: "While consumer applications such as fitness monitors and self-driving cars attract the most attention and can create a significant value, our analysis shows that there is even greater potential value from IoT use in business-to-business applications. In many instances, such as in worksite applications (mining, oil and gas and construction), there is no direct impact for consumers."

McKinsey estimates that up to 70% of the value the Internet of Things is expected to generate in 2025 will come from B2B use of data. However, it will not be without the use of personal data and will not be entirely unproblematic, because the value in some cases is estimated to be even higher if personal data is combined with B2B data. Employers could, say, monitor their employees' blood pressure or blood sugar to keep them optimally 'maintained'. But in terms of B2B data, the biggest headline is the fact that data can optimise production and be used for 'predictive maintenance'. By way of a real-life example, Harley Davidson has a system which automatically adjusts to humidity and other conditions so that their motorbikes are coated with perfect enamel. On the topic of predictive maintenance, McKinsey describes how a company could prevent the collapse of a produced item due to damaged parts by monitoring the machines in real time and repairing parts before they break.

Vestas. The Danish wind energy company Vestas – the largest provider of wind turbines in the world – is a frontrunner when it comes to the use of big data. Before Vestas built its supercomputer with 15 years' worth of data on wind and weather, it could take up to 18 months to erect wind turbines which were optimally positioned in relation to wind and wind production. Today, Vestas uses an algorithm to create a statistical basis for decisions regarding the layout of wind turbines; the work is done with the click of the mouse. Drawing on data from 35,000 public stations which supply measurements

on over 150 parameters about every 6 hours, Vestas can produce accurate forecasts for long-term energy production at any point on the globe. Big data is also a part of their ongoing service. Sensors on individual wind turbines along with weather data are used to predict the wear and tear – and plan for the turbine's upkeep.[8]

Food Genius. This company delivers trends and data analyses to the food industry and is built entirely on big data. It retrieves data by scanning more than 87,000 menus from more than 350,000 American restaurants for a total of 50 million meals. This allows the company to analyse the diffusion and use of certain foods and menus as well as facts about individual ingredients, cooking methods and food types, such as organic or spicy dishes. The food industry uses the service to adjust production, develop and name new products, or change the menu.[9]

Enevo. Based in Finland, this company has developed algorithms which can foster more efficient waste collection in smart cities. Sensors inside the garbage container lid measure how full they are, so drivers don't use fuel in vain to empty half-full containers. By analysing the data collected from the sensors, Enevo can predict when containers are full and empty them accordingly. The stated objective is both environmental and economic, and so far the company's pilot tests in Helsinki and London show between 50% and 90% savings on driving, depending on the efficiency of the existing waste system.[10]

8. Datadreven vækst i Danmark, p. 16, IrisGroup, 2014.

9. Datadreven vækst i Danmark, p. 23, IrisGroup, 2014.

10. Harddisken, P1, DR, 2015.

iCow. Thousands of small cattle farmers in Kenya use the app iCow to optimise milk production. This program was invented by Su Kahumbu and provides the farmers with information about their cows' oestrous cycles, milking and market data.[11] In practice this means, for example, that the farmer receives a text message on the day the cow is the most fertile. The app collects the farmer's milk production and breeding data and sends him updated personalised advice and best practices via text messages, while simultaneously providing information on milk demand, veterinary data and market prices.

A growing number of organisations are developing methods to use big data for social or scientific purposes. They face similar ethical challenges as companies do, since they collect and store sensitive data, like that relating to health and location. Humanitarian organisations are using big data to trace the spread of a disease across a continent or to assess where to place aid centres. Big data is also used in food and medical research or to optimise the efficacy of hospitals.

Although the idea of using big data for humanitarian or scientific purposes is fundamentally different than the idea of profiting from its commercial use, the privacy risks are similar. In the report *Ebola: A Big Data Disaster*[12], Sean Martin McDonald explored the use of big data in humanitarian crises and the privacy implications for some of the world's most vulnerable citizens. As stated in the report, big data was even used to perform migration analysis and contact tracing without user consent during the 2015 Ebola outbreak in West Africa.

UN Global Pulse. Global Pulse is a big data innovation initiative from the United Nations. Its mission is to accelerate the discovery, advancement and scaled adoption of big data innovation for sustainable development and humanitarian

11. Udder genius: Fellows Friday with Su Kahumbu, 2012.

12. The Centre for Internet Society, 2016.

interventions. The initiative emphasises safety and responsibility, with a department dedicated to 'data privacy'. Global Pulse consists of a network of innovative labs and partners with experts from UN agencies, governments, academia, and the private sector conducting research in the field and developing new approaches and methods.

Just like some humanitarian organisations are exploring ways to use big data on individuals while respecting their privacy, a number of for-profit companies are also exploring ways to use big data without it pointing back to individuals. The focus here is effective anonymisation and secure storage.

Movvo is a Portuguese company that capitalises on location data. Movvo collects consumers' movements around shops with antennas installed in shopping areas. They then analyse the data and sell the results to retailers seeking to understand how consumers move around shops and cities. The company claims not to know who owns the mobiles they download data from, that they receive only a unique encrypted radio signal and that all data is anonymised. To gain trust from the public, Movvo obtained the Europrise privacy seal, which originally was established by the German national authorities and later privatised.

There is an embedded risk in collecting, storing and processing masses of personal data. Even when data is anonymised, the possibility of identifying individuals still technically exists if the data set is large enough. Some data which is not personal per se, can become so when correlated with other types of information. For example, if enough data is linked to Apple addresses that are in turn linked to individual consumer devices (Wi-Fi or Bluetooth identifiers), it is technically possible to use these identifiers to reveal who that individual is. For this reason, many companies are working on ways to use big data without compromising personal privacy. One of these is 'differential privacy', a

method which uses data hashing and noise injection to enable analytics on big data while keeping personal data private. In 2016, Apple stated that they plan to implement differential privacy for their services.

There are many good examples of using big data to support research and progress in developing countries, to streamline processes in factories and the like. Ultimately, challenges to privacy are often posed by the data collection and analysis' scope and, as follows, the proprietary context, how data is protected, and how it is stored and anonymised.

DATA AT RISK

The collection and storage of large quantities of personal data is in itself a risk to individual privacy. As such, data protection legislation in Europe prohibits collection without a specific purpose and requires user consent. However, the analysis and use of said data is, in particular, a challenge to individual rights. Algorithms are designed to make sense of data; algorithms are the foundation for data-driven services and the creation of profiles to personalise marketing and content, among other things. An online service can target advertising and content based on a person's preferences, previous patterns of consumption, and socio-economic background. These profiles can be so fine-tuned that they reveal intimate, private details, such as pregnancy or the likelihood a couple will get a divorce.

It goes without saying that there are ethical implications associated with the algorithmic analysis and use of data.

There are numerous examples of dilemmas to be found in the wake of algorithmic prediction, which may create opportunities or limitations for an individual. Algorithms and their design criteria have a direct impact on an individual's opportunities when, for instance, American prisons use predictive algorithms to calculate the probability that a

person will commit a crime again after his or her release from prison, based on various social and behavioural data on the detainees. The same goes for the use of algorithms by employers to match a potential job applicant's social media history with the company culture. For example, what are the selection criteria and which cultural and social indicators does it base its selection on? Are they biased? What are the privacy implications?

A risk analysis of the use of big data has been described by Professor Frank Pasquale in his book *The Black Box Society*.[13] He explains the effect of hidden algorithms acting on our digital data. These calculations can create or destroy one's reputation; they can determine a destiny. We do not, he argues, have insight into the motivations and intentions that lie behind them. We don't know how personal data is used, for what purpose and what the consequences will be for the individual.

Facebook's Newsfeed is an instance of the use of a black box algorithm according to a background paper produced for the government-funded Global Conference on CyberSpace (GCCS) in 2015.[14] Facebook's algorithm determines what you see on your wall and what you do not see. It's then adjusted by a team of researchers, who say they take thousands of factors into account. In 2016, it emerged that a small team of editors was actually injecting news topics into those trending among Facebook's users or into its 'blacklisted' topics. A Gizmodo blog claimed that this conduct was biased against conservative news items.[15] Facebook immediately rejected the claim, but it does not change the fact that what is presented as news to Facebook users is in no way a neutral presentation of accumulated user-generated content

13. The Black Box Society - The Secret Algorithms That Control Money and Information, Frank Pasquale, Harvard University Press, 2015

14. The Ethics of Algorithms: from radical content to self-driving cars, Centre for Internet and Human Rights, 2015.

15. Facebook's News Selection is in the Hands of Editors not Algorithms, Documents Show", The Guardian, 2016.

and interest in current events. Rather, it's a combination of algorithms and human editorial intervention, where the criteria and the processes behind such opaque editorial decisions are kept secret.

> **Target**. In 2011, the American discount retail chain Target developed an algorithm capable of finding customers who were about to become pregnant and even approximate their due date.[16] The chain could then directly market their baby and pregnancy products to these customers. The programme was so successful that the sale of products for pregnant women increased up to 30%. However, there was a problem: the creepiness factor. One day a furious father stormed into a Target location to complain that the store was sending pregnancy product adverts to his 16-year-old daughter. It was as if they wanted her to get pregnant. What he didn't know was that his daughter was already pregnant. The pregnancy algorithm knew before he did. A few years later, data on up to 70 million customers was stolen from Target, resulting in a major security breach and a sizeable economic loss for the chain.

It's not only risky for individuals to lose control over their data, data is also a risk for a company if not handled with due diligence and appropriate care.

> **Nets / IBM / Aller**. To many people's great astonishment, Danish publisher Aller's weekly tabloid, Se & Hør, managed, week after week, year after year, to reveal the buying habits and whereabouts of Danish celebrities, including the Danish Prime Minister Lars Løkke Rasmussen and the world famous actor Mads Mikkelsen. In April 2014 it was revealed that an IBM employee had been regularly texting data on Danish celebrities' credit card use to the tabloid's staffers. IBM was a subcontractor

16. How Companies Learn Your Secrets, New York Times, 2012.

of Nets Holding A/S, a payment and credit card service provider for all electronic money transfer methods in Denmark. As one of the small country's biggest privacy scandals, it gravely damaged the reputations of all three companies. In the end, it cost Aller a large amount of their readership and in 2015 the media organisation was reported to have lost more than 4 million euros.[17]

Mozilla. The owner of the popular Firefox browser promoted one of its best data analysts, Brendan Eich, to CEO in 2014. Six years earlier, Eich, who also co-founded Mozilla, supported an anti-gay marriage campaign with a contribution of $1,000. Back then the majority of Americans, including Obama, were against same-sex marriage. But by 2014 the national mood and opinion had changed, and when Eich's contribution came to light, the pressure against him became too heavy. He lasted just 11 more days as CEO, and Mozilla is now a cautionary tale of how vulnerable companies become if their employees do not also take care of their digital reputation.[18]

Samsung. In February 2015 a story about Samsung's Smart TV went viral.[19] 'Samsung spies on you', was the message. Journalists had been looking into the company's privacy policy and discovered that all conversations in the room where the TV was located were being recorded and processed by the company as part of a speech-to-text conversion service. The conversations were digitally delivered to a subcontractor to be processed into text form. Though it was unclear whether it was an opt-in or opt-out option, the viral discussion was incredibly unfavourable

17. Se og Hør sagen har kostet Aller 30 millioner, Berlingske Business, 2015.
18. How Mozilla Lost Its C.E.O., The New Yorker, 2014.
19. Your Samsung Smart TV is Spying on You, The Daily Beast, 2015.

for Samsung, which in the end responded with a 'we take privacy very seriously'.

DATA BROKERS IN A GREY AREA

There are plenty of examples of companies running into problems because they lacked control over their data and it's only a matter of time before more scandals emerge. Security breaches aren't only a threat caused by hackers from the outside or employees compromising data from within, harbouring direct criminal intent. Many companies also operate in legal and ethical grey areas in terms of what they can and cannot do with data. Insurance companies monitor customers and their data to reduce damage claims in court and assess their customers' health and behaviour to then adjust their insurance premiums. Airlines, car rental agencies, bookstores and many others establish prices based on knowledge about customers obtained by using cookies and other tracking tools. Many businesses both buy and supply data to the infamous multinational data brokers, companies that deal in personal information and which haunt the US in particular – or at least they're identified in the United States.[20] To illustrate this point, at the end of 2013 the director of the World Privacy Forum, Pam Dixon, disclosed that data brokers sell lists of chronically ill people, cancer patients, rape victims, alcoholics and the homeless to the pharmaceuticals industry.[21]

20. Data Brokers a Call for Transparency and Accountability, FTC, 2014.

21. What Information Do Data Brokers Have on Consumers, and How Do They Use It?, Testimony of Pam Dixon Executive Director, World Privacy Forum Before the Senate Committee on Commerce, Science, and Transportation, 2013.

A NEED FOR NEW BUSINESS MODELS

Throughout the history of the Internet, personal data (our location, identity and social conditions, consumption and behavioural patterns, desires, needs, interests) has been in the pipeline as part of a greater business movement focusing on direct marketing and personalised services. It's in this context that big data's potential has been somewhat misinterpreted as specifically associated with the storage and processing of personal data.

Erik Huizer[22] is CTO at the Dutch SURFnet. He was part of the web's infancy as both a developer and entrepreneur. His name is listed in the Internet Hall of Fame, which honours those who had a particular impact on the Internet's development. On the data-driven business model's development, Huizer had this to say:

"Nothing went wrong intentionally. People just started experimenting with it. People didn't mind giving away their data because they thought they were doing it in very specific contexts. To share information with people they knew. And then somebody else got the idea 'what if we combine this with other data?' This of course changed the whole privacy context without consent. They developed a business model without considering what this meant to privacy in general."

In the beginning, entrepreneurs and companies saw data as a monetary object, something that users needed to pay with in order to use their services. They didn't care about privacy. Later, there came a time in which companies said they did indeed care about user privacy, which, according to Huizer, was not very convincing as they were simultaneously collecting hordes of data on them. Today he cites a new, emerging trend in the Internet's technical and commercial development:

"Now we see the emergence of new companies that take privacy as a starting point. They structure their businesses from the beginning to acknowledge privacy and deal with privacy. Their business model is

22. Erik Huizer, November, 2015, personal interview.

based on an awareness of a backlash against the data monetising business model where users increasingly will flee towards their platforms. I've seen that movement over time."

The predominant digital business model, based on the raw harvesting and use of personal data mainly for the benefit of shareholders, is not only likely to have reached the lower limits of consumer confidence and corporate reputation. The model is also threatened by a growing number of users knowingly providing false data in the form of fake names, birth dates and spam email addresses in order to protect their privacy.

In the hunt for web traffic and downloads from new customers, a whole new industry has emerged (and is especially flourishing in Asia) which can supply anything that appears to be user activity. Some studies show that over 60% of all traffic never sees human eyes but is rather so-called bot traffic generated by computer programs, and that 90% of a company's marketing budget for online advertising is simply wasted.[23] With this knowledge, it is clear that we need to look for different business models in the digital world. Fortunately, there are more and more companies taking a few for a test drive.

23. The Alleged 7.5 billion Fraud in Online Advertising, Samuel Scott, blog 2015.

People are not just concerned about the surveillance capabilities of new technologies. They are also starting to act to actively avoid it.

CHAPTER 3

WHAT CUSTOMERS WANT

Many websites greet their customers and potential customers with personal messages, offers and prices. Some find it helpful, others intrusive. Personalisation is based on our digital footprint, but it feels particularly intrusive when someone holds and uses sensitive personal information about us without our knowledge. It feels like a betrayal of trust. Advertisements appear on your Facebook wall for things you don't remember ever having shared on Facebook – diapers, Alzheimer's, offers of assistance from a divorce lawyer or dating opportunities. Or what about the pair of boots or travel destination that continues to chase you around the web, even if you've already purchased them or have long since found an alternative holiday destination? And what about the price you paid for the rental car, hotel, flight or book. Are you sure you got the best price? Why did it rise the second time you came around? Perhaps others got it for less?

Most people would like to decide for themselves just who knows exactly what about them and when. At a flea market we bargain about the price, but online the playing field is uneven. The seller often knows more about the buyer thanks to intense data collection. In the era of big data, there's been a shift in the control over information about us. We have less oversight and less control of the data that forms our digital identity – personal information such as name and address, diseases,

needs, dreams, data on our family and network of friends, our motivations, patterns and habits. This lack of control is something consumers are beginning to feel directly and respond to. In an online environment, trust between a company and its customers is delicate, and thus a long term strategy must leave space to listen to consumers' concerns, observe their actions and react in good time.

GENERAL CONCERN FOR DIGITAL SURVEILLANCE

There's a movement going on among Internet users which comes to light by comparing studies, statistics and trends: they're beginning to demand control over their data. Several studies asking Internet users directly about the importance of privacy, data security and control suggest that they place these things high when ranking digital needs. Though a global trend expressed differently from region to region, it's particularly evident among consumers in the US and Europe, where the digitalisation of public services and use of digital media is high and where data leaks and surveillance scandals have been in the public eye.

Generally speaking, there has been a change in how the world's citizens perceive challenges and risks to their privacy.

While privacy violations traditionally have been linked with state-sponsored surveillance activities, many have also begun to worry about private companies' personal data collection.

A global CIGI-Ipsos survey[24] from 2014 showed that 74% of people from different countries in various continents were concerned that private companies monitor online activity, collect data and resell it. Much of this concern is associated with a lack of transparency in corporate data use and, consequently, consumers' lack of control over their personal data. Another survey which covered over 8,000 con-

24. CIGI-Ipsos Global Survey on Internet Security and Trust, November 24, 2014.

sumers in five countries (USA, Canada, UK, France, and India) from the Columbia Business School/Aimia[25] showed that 85% of people wanted to know more about what the collected data is used for, 86% wanted greater control over their data, and 80% would only provide their data to companies they believe they can trust.

On this topic in Latin America, Eduardo Bertoni[26], Director of the Center for Studies on Freedom of Expression at the Universidad de Palermo in Buenos Aires, stated: "There is a similar concern as in Europe regarding corporate surveillance. It varies from country to country. But people are starting to think that the main actor that affects their privacy is not the government, but the business sector. Most people see the private sector as a foreign power spying on them. This is also connected to an increasing mood of anti-imperialism. If they see a US company doing something in their country, true or not, they see it as a foreign state in their country."

In other regions, the trend is less clear. Such is the case in the Middle East, where basic access to online services often take priority over the right to privacy. Hanane Boujemi[27], Senior Manager of the Internet Governance Programme for the MENA Region at Hivos, says that many respond with a shrug to stories of commercial and governmental digital surveillance. "The interest in the Middle East in the concept of privacy is not as big as in the European region. They are used to surveillance. It is something that is lived on a daily basis for these people."

Concerns about commercial surveillance are strongest among consumers in Europe. Here, the vast majority of citizens accept that data collection is part of the digital business model and a prerequisite for gaining access to many digital products and services. In fact, 71% accept this condition according to a Eurobarometer survey from June

25. What is the Future of Data Sharing?, Mathew Quint and David Rogers, Columbia Business School, Aimia, 2015.

26. Eduardo Bertoni, November, 2015, personal interview.

27. Hanane Boujemi, November 2015, personal interview.

2015.[28] But at the same time, only 31% feel they have control over their data and a solid 67% of those surveyed are concerned about lack of control. The Eurobarometer survey, which included 28,000 Europeans, also showed that:

- 7 in 10 people are concerned that their data could be abused or that it will be used for purposes other than what it was collected for.
- Half of survey respondents said they partially read privacy policies, one third said they never read them, while only around one in five reads them thoroughly.
- 7 in 10 people also say that privacy policies are generally too long, and 4 in 10 people find them too difficult to understand.
- A large majority of Europeans expressed the belief that a company must always obtain explicit consent to use their data.

WHO DO INTERNET USERS TRUST?

Surveys in Europe and the US show that Internet users mostly trust regulated industries over non-regulated industries. Hospitals, banks and, partly, insurance companies are high on the trust scale. Search engines, social media and news media, on the other hand, are often the industries that Internet users trust least.[29]

TARGETED ADS AND PRICES

While some consumers appreciate targeted advertising that matches their style and interests, others don't care for it at all. One thing is certain; personalised content and offers are here to stay, and many com-

28. Special Eurobarometer 431 Data Protection, EU Commission, 2015.

29. State of Privacy Report, Symantec, 2015.

panies are trying to follow in the footsteps of Amazon and Netflix, experts in the delivery of what they call 'relevant' recommendations.

There's a great degree of variation in what consumers say when asked if they want targeted advertising, but often the answer depends on the way they are asked. According to Eurobarometer, 4 out of 10 are okay with the fact that companies use knowledge about their online behaviour to tailor advertisements and content. When respondents to a survey from the Danish Business Authority and The Danish Society of Engineers were asked similar questions, but with more specific information on the tracking processes that led to personalisation, they were much more sceptical. 'Is it a good use of cookies to give you personalised offers from the page you visit?' Only 24% answered yes. 'Is it a good use of cookies to give you personalised offers from other websites you visit (meaning that the advertisement follows you from other sites)?' Only 10% answered yes here.

A Norwegian study asked directly: 'Do you prefer targeted advertisements? (27%) or random advertising (73%)?'[30]

Evidence suggests that personalisation quickly gets to the point of feeling like manipulation, and consequently a company should use it with caution.

TEENS WANT PRIVACY

There has been a tendency to attribute concerns over privacy to the older generations' perception of the role of privacy in society. But young people actually place much more value on their online privacy than many adults think. They're frustrated by the lack of transparency in what data is harvested and why, and resentful of the lack of control they have when that data is used in targeting activities which are seen as invasive and irritating.[31]

---

30. Personal data in exchange for free services: an unhappy partnership?, Norwegian Data Protection Authority, 2016.

31. See e.g Youth State, survey on UK 16 - 24 year olds from Adjust Your Set.

Detailed studies on young people's use of digital media show that privacy is alive and kicking. Danah Boyd, an American researcher and founder of Data & Society in New York, came to this very conclusion. According to her, young people draw upon a wealth of complex strategies to maintain privacy on social media. They do actually want to keep some things to themselves, even while social and active online. Boyd has appropriately named the kind of privacy young people manage on social media 'social privacy'. In the minds of this demographic, privacy is connected to social context. For example, if an image from a social networking profile is taken out of the context it was posted in and used in a different context, many will see it as a violation of their privacy. Even if they have originally shared it in a place where everyone has access to it.[32]

Millennials are in fact quite aware of their privacy on social media. For them, privacy is not about closed boxes with locks and keys, but about being in control. They know that having a private life online means having control of the social context things are shared in. The great lengths they will go to in order to hide things from their parents online is proof of this. Studies also show that their views on privacy change according to their needs.

Once they enter the labour market, it's no longer just parents, friends and teachers. Suddenly, those who they must shield certain information from expands to include potential employers and others.

A majority of young Germans between 18 and 29 years old (54%) are against online policies that require that you use your own name when leaving comment, while 81% of the over-59 German demographic finds them quite okay.[33] In fact, there is a rather large opposition to sharing personal data with companies among young adults. Nine out of ten youths in the UK, for example, do not give away their

32. Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life, MIT Press, 2007.

33. Most Germans in favour of compulsory real names online, The Local De, 2016.

data no matter the benefits, according to a KMPG survey of 18 to 24 year olds.

DEMAND FOR DATA CONTROL

Young peoples' experiences navigating online identity, privacy and social networks provide an important insight into future market requirements and drivers of innovation.

It's not just the youth who want to be empowered online. Generally, consumers are demanding more and more control over their data and their digital identity.

First and foremost, consumers need to feel that a company is able to take care of their data. If so, they are more willing to share data with the company. This confidence in the security of data held by tech-based services is in many cases more important than good customer service or customer discounts. Consumers wish to be informed when their data is stolen or lost, though too few feel they are kept in the know. A majority of Europeans do not feel sufficiently briefed about what their data is actually used for when requested by a website. The facility to revoke permission – to delete data – is identified as the single largest factor in encouraging consumers to share more.[34]

A digital trends report from Microsoft Advertising[35] looked at the consumer motivations which drive online behaviour in different regions of the world. It shows a growing desire among consumers to control their digital identities. For example, 57% want to be able to choose how long information they share stays online and 80% are interested in services that 'manage their digital identity'. It is, as the report states, a shift from a consumer focus on privacy as a way to hide

34. Fair Trade?, Amazeone.com, Sarah Hooper, Paul Kennedy, 2016.

35. Microsoft Digital Trends 2015 - The evolution of digital consumer experiences, Microsoft Advertising.

digital footprints, to a focus on control of data and thus of one's digital identity.

CONSUMERS ARE BEGINNING TO ACT

In May 2014, the European Court of Justice passed down a judgment that is already playing a crucial role in the individual right to control personal data and privacy. With what is referred to as the right to be forgotten, Google and other search engines were asked to process requests to remove links to content and actually delete those deemed irrelevant, false or outdated. Google and a number of other tech and media companies immediately went out of their way to criticise the decision, saying it would have a negative impact on freedom of expression and provide criminals and public personages an opportunity to have content removed that could be in the public interest. However, contrary to the many warnings, it turned out that 95% of all requests to remove links came from ordinary people, not from criminals, politicians or public individuals. In countries like France, Germany and the Netherlands, 98% of all requests were based on privacy concerns.[36]

BLOCKING COOKIES AND USING VPN

The right to be forgotten is one thing. The right not to be monitored or tracked by companies is yet another. The current digital business model, tracking-by-default, means that individuals have to take action if they do not want to be monitored and receive personalised advertisements and prices based on their data. A rapidly growing number of users are starting to act. For example, millions of Internet users are blocking online adverts with adblockers, such as AdBlockPlus or AdblockFast and cookie-blockers such as Disconnect.me. Especially in the Western world, a large amount of people use blockers (the lowest per-

36. Google Accidentally Reveals Data on 'Right to be Forgotten' Requests, The Guardian, 2015.

cent in Ireland, the highest in Sweden and Germany), and this new blocking trend is considered a serious threat to the ad-based business model. Millennials are especially adept at using ad blockers. According to a US survey carried out in autumn 2016, two out of three between 18 and 24 years old used them.[37]

More and more are starting to use VPN services also. They encrypt web traffic, so it's safe to work on a free and open Wi-Fi-connection, and they allow users to hide or select the origin of their IP address. According to a GlobalWebIndex survey from 2015, one in four have used a VPN service. However, this is not necessarily because it protects privacy, but also because it can provide access to film streaming services worldwide.

FALSE DATA ON THE RISE

Another way to protect one's privacy is to provide false names and data online, to use a pseudonym or an alias. More and more people are doing this, and the younger you are, the more you do it. Companies like Facebook and Google have real name policies (Google abolished its real name policy in 2014), which means that their Terms of Service (TOS) requires users to provide authentic data. If you don't heed these conditions, the greatest risk you run is that your account will be closed. At least 20% of account holders (Facebook's own figures) use names other than their own. This could be anything from political activists and transsexuals to CEOs and people who just want to be left alone. False data is used not only on social media, but also in surveys, particularly when one has to fill in fields to get a report on a website, participate in prize drawings, and the like.

In the UK, up to 60% of users intentionally entered incorrect personal data about themselves, such as a false date of birth, email, name and address, according to a survey among consumers by the research

37. Millennials At The Gate, Anatomy Media, Fall 2016.

company Verve.[38] Eight out of ten users cited concerns about privacy as their main reason, but many also said that they want to stop companies from sending them targeted advertisements. In another study, which looked at Internet users in eight European nations (Symantec's The State of Privacy, 2015), one in three people lied online to protect their privacy.

OBFUSCATION

As part of the fake data trend, we also see attempts to drown true data in fake or 'dirty' data. In their book, *Obfuscation*[39], American professors Finn Brunton and Helen Nissenbaum describe a consumer revolution based on the conscious use of confusing, misleading and false information to prevent surveillance and data profiling. To address this, they created the browser add-on TrackMeNot. It drowns internet users' actual queries on engines such as Google, Bing or Yahoo with a long strip of ghost searches. The same with AdNauseam, which Nissenbaum is also behind. When you go to a website, everything on the site is automatically clicked, drowning the actual behaviour of the user in hundreds of clicks. According to a global Aimia-survey[40] of 8,000 consumers in October 2015, 67% have done something to protect their data – including providing companies with fake data.

FROM LACK OF KNOWLEDGE TO RESIGNATION

There is still a great lack of knowledge among consumers about what is really going on with their data. In a Harvard Business Review study[41] of consumers in five countries (USA, UK, China, Germany

38. Consumers are Dirtying Databases with False Details, Marketing Week, 2015.

39. Obfuscation: A User's Guide for Privacy and Protest, MIT Press, 2015.

40. How Business Can Gain Consumers' Trust Around Data, Forbes, 2015.

41. Customer Data: Designing for Transparency and Trust, Harvard Business Review, Timothy Morey, Theodore "Theo" Forbath, Allison Schoop, 2015.

and India) from 2014, only 25% knew that their digital footprints revealed their location, and even fewer were aware they also contain searches and Web browsing history. Symantec's State of Privacy 2015 survey stated that nearly seven in ten people don't know how to protect themselves against surveillance.

Now, one would think that more knowledge would lead to action. Not necessarily. The Tradeoff Fallacy[42], a survey from the University of Pennsylvania in June 2015, showed that nine in ten Americans do not think it's a fair deal to pay with their data for a digital service. It was assumed previously that many people gave their personal data to companies because they were unaware of what was happening with it. Yet this study shows that the opposite can happen; that those who know what is happening with their data are actually more likely to accept a discount in return for providing their data. Why? Because, concluded the authors, they are acting with resignation in relation to being in control. Resignation happens when a person believes the undesired result is inevitable and when they feel powerless to stop it. So rather than being empowered by the knowledge of their data transactions, some feel it is pointless to try to gain control of the situation. Though ultimately, more than half wished they had never lost control in the first place.

PAY FOR PRIVACY

Working at Carnegie Mellon University, Italian professor Alessandro Acquisti has made a career out of studying online consumer habits and their so-called 'privacy tradeoffs'. In a series of experiments, he looked at the value people attach to their privacy when presented with the choice to pay for its protection in different ways. His conclusion was that there's no evidence showing that consumers generally don't care about their privacy. The value they attribute to their privacy is complex and subject to a variety of factors, such as their personal motiva-

42. The Tradeoff Fallacy, Joseph Turow, Michael Hennessy, Nora Draper, 2015.

tions and the way choices are presented to them. In one study, for example, he investigated if consumers would pay for privacy.[43] Participants were asked to use a specially-designed search engine to buy a pack of batteries or sex toys with their credit cards. When the search results only listed the online shops, the subjects were not interested in the privacy policies. They simply bought only the cheapest products. But if the search results also showed comprehensible information about the differences in the online shops' privacy protection policies, the participants paid 5% more on average for products from those with the highest level of privacy.

In other studies[44]shoppers in a department store could choose between receiving an anonymous gift card with 10$ for purchases and a gift card with 12$ that tracked purchases. Here, those given advance notice about the better privacy protection their choice would imply if they chose the card with less money for purchases, would be five times more likely to take this card than others without this awareness.

There is no doubt that a company is better off protecting its customers' data and only using it for specific purposes rather than disclosing, sharing or selling it to third parties. It's a personal arms race and certainly the companies that collect data and use it in a lawful and ethical manner will be tomorrow's winners. Ad and cookie blocking, the use of VPNs, and fake data are clear threats to the tracking-by-default business model. Effective ad and cookie blockers are significantly on the rise, as they are easy to use and may have obvious economic benefits, particularly if you know how to fool a website into thinking that you are a first-time user. The use of fake data will also grow, as we see it used among millennials. There is a gap between what consumers want – openness and knowledge about the use of their data – and

43. The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study, Janice Tsai, Serge Egelman, Lorie Cranor, Allessandro Aquisti, Weis, 2007.

44. What is privacy worth?, Alessandro Acquisti, Leslie John, George Loewenstein, The Journal of Legal Studies, Vol. 42, No. 2, The University Chicago Press, 2013.

what they see businesses doing. Long, incomprehensible privacy policies where users lose their right to control their data without fully understanding what it is they are accepting is an absolute no-go. As with the environment, consumers will realise that they must do something to gain control over their digital identity, causing a rise in demand for privacy-enhancing products and services.

Visionary companies are taking extra steps to safeguard privacy, to secure and protect data in order to build trust among their customers.

CHAPTER 4

DATA ETHICS FACILITATES TRUST

When you walk into a grocery store, you have all the tools necessary to choose between the wide range products for sale. Quite literally, you can pick whatever you want to buy and read through its ingredients and nutritional facts. You trust that the milk you're buying won't make you sick. Rarely do we stop and think about the machine behind the system of trust indicators that surround us when we decide what to put in our grocery basket: legal requirements regarding ingredients, globally-negotiated health standards, etc., all embedded in the item's production chain. We trust there is a formal system in place to manage the risks. We delegate trust, so to speak.

In today's data era we are seeing the creation of a new trust system to manage the risks of a data-saturated environment. New requirements regarding businesses' treatment of personal data are embedded in laws, global ethical standards are created, verification systems for customers are emerging. Cutting-edge companies are already responding to this ongoing global negotiation of standards, roles, rights and responsibilities. They're building their customers' digital trust.

Churchdesk. When Churchdesk wanted to export its platform for churches to Germany, they were asked where they stored their data. Like so many others, they had chosen Amazon Web Services (AWS), which is functional as well as cheap. But the

Germans wouldn't accept that. And the argument that it was Amazon Ireland, in Europe, didn't help. No, the data needed to be stored in Europe by a company with European headquarters if the Germans were to buy the platform, which contained sensitive data of a religious nature on citizens. So Denmark-based Churchdesk moved their data from Amazon Ireland to a more expensive German cloud service, T-Systems. At the same time, they had to certify their workflow concerning data and they ended up with a large bill in order to meet the German demands on data protection. It turned out to be worth every penny, they say[45], for data protection quickly became a competitive parameter for Churchdesk in Germany and later in the UK.

LEGO. Over 50 million children play in LEGO's online universes. When they log on to services that require parental consent, they use LEGO ID. At first LEGO considered using social media connect buttons because many children already were on social media platforms, but in the end the toymaker chose not to as it was unable to get assurances from such platforms as to what type of data would be reaped from its sites. LEGO says it has a corporate responsibility as to how subcontractors and partners use data of its customers, just like the company is accountable for its physical suppliers' environmental and social behaviour. As a result, there are no third party cookies on LEGO websites aimed at children under 13 years. LEGO says it wants to be in control of what happens to its customers' data. Free third party analytics tools are not used and all data is stored in Taulov, Denmark (with the exception of the data pertaining to Russians, because of legal requirements to store their data in Russia). With a mix of users that also includes minors below the age of 13, LEGO adheres to

45. CEO and founder Christian Steffensen, March, 2016, personal interview.

the US COPPA regulation aimed at protecting children (similar rules on age limitation are introduced in the GDPR from 2018). They also encourage children to use pseudonyms as an additional way to protect their identities.

TomTom. Location data or GPS data is personal data. The Dutch company TomTom, which sells GPS hardware and software for self tracking (e.g., for fitness watches) and for cars is differentiating itself from its competitors by building privacy protection into its products. For example, TomTom promises to delete all data that would make it possible to identify you or your device from the location data they receive within 24 hours after your device is powered off. In its privacy policy the company claims to not know where the user has been and to be unable to tell anyone else this, even if forced to.[46]

Churchdesk, LEGO and TomTom are examples of companies that have taken an extra step to cultivate their customers' trust around the treatment of their personal data. They are reflective of dataflows and restrict it to stay in control, even informing their customers about it. Rather than an obstacle, data protection and privacy are seen as competitive factors by these companies.

"We can see that data protection is more and more sought after, so it's a competitive advantage," said Dieter Carstensen[47], head of digital child safety at LEGO. "Our top management has decided and fully support our restrictive rules on the use of personal data – even if in the short term it may have an economic impact on LEGO."

Other players in the field have gained experience the hard way. In September 2016 Viacom, Mattel, Hasbro and JumpStart agreed to pay a total of $835,000 in violation of the Children's Online Privacy

46. Privacy Policy, TomTom.com, 2016.

47. Head of Digital Child Safety, Dieter Carstensen, January, 2016, personal interview.

Protection Act for tracking the activity of and collecting personal information on children under the age of 13.[48]

DIGITAL TRUST

"Trust is beautiful", according to Neil Richards and Woodrow Hartzog.[49] Trust is the foundation of our relationships in a digital society and the treatment of privacy is the balance established between companies and people. The problem is, they argue, that we do not understand privacy as an issue of trust, only as a matter of protection, compliance and administrative burden. Rather than being 'privacy pessimists', we should be 'privacy optimists' and see privacy as a way to build trust. The way we approach and handle personal data and privacy is a core trust indicator.

Trust is a prerequisite for the establishment of a digital relationship be it two people communicating with each other, between a publisher of information and their readers, or between a business and a consumer. The Internet has made our world smaller; we can interact with several different companies, institutions and people, and establish relationships across great spatial distances. It's a phenomenon that, in 1990, geographer David Harvey called 'Time-Space Compression'[50]: the result of a technological development that reduces spatial and temporal distances and, so to speak, compresses the space we move around in. Distance is also what has made trust a key prerequisite for online interactions where determining authenticity is a core issue. One simple example is online shopping. You, as a customer, do not have the same opportunity to confirm a service's authenticity as when you step into a physical store, where you can see and 'feel' the people and organisation you are dealing with. Studies show that consumers' digital trust is at its lowest when it comes to online shopping.

48. Popular websites fined $835,000 for tracking kids online, CNET, 2016.

49. Taking Trust Seriously in Privacy Law, Stanford Technology Law Review, 2015.

50. The Condition of Postmodernity, Blackwell Publishers Ltd, 1990.

THE SNOWDEN EFFECT

The term 'Snowden Effect' has been used to describe the large scale political, cultural and economic fallout after American whistle-blower Edward Snowden's mass surveillance revelations in June 2013. Although not in agreement on its concrete manifestations, there is one thing politicians and industry representatives around the globe agree on: The revelations on programmes such as PRISM, which illustrated US intelligence's access to American social media services, caused a digital trust crisis.

Tech monoliths Facebook, Apple and Google saw this immediately and were the first to attempt to reassure their users in order to restore trust in their services. They immediately denied all knowledge of the PRISM programme. Google founder Larry Page responded quickly with a surprised blog post titled 'What the ...?', and later with a more official statement that emphasised a very personal style of customer relations: "'Google cares deeply about the security of our users' data...". Page and his company were clearly aware that the trust-based relationship created with users had been severely damaged. Aol, Apple, Facebook, Google, Microsoft and Yahoo, along with other US companies and organisations, then wrote a letter to President Barack Obama, where they asked to be allowed to publish the specific figures on requests for personal data on their users under the US Patriot Act and the Foreign Intelligence Surveillance Act (FISA). To them, trust is about creating transparency for their customers concerning their interactions with the US government. Through this transparency effort, they hope to reduce the distance the revelations created between them and their customers – but without reducing their own access to and capitalisation on that same personal data.

THE SHARING ECONOMY

Trust is profit. Quite literally. It's the business model for Internet companies like the private home rental service Airbnb, the platform where you can hire people for smaller jobs and tasks TaskRabbit, the carpooling service BlaBlacar or GoMore and many other companies like these which form the sharing economy. Their business is to mediate trust between private individuals by giving them the tools to verify or to create expectations about each other and the products and services they use.

Rachel Botsmann, the woman behind the 'collaborative consumption' concept, speaks of 'reputation capital'.[51] That is, the value of one's reputation in this new type of collaborative sharing economy. She uses the example of a landlord on Airbnb, who got a cat to avoid getting a bad review from a guest who had seen a mouse running across the floor in the apartment he was renting. In the sharing economy, private individuals trade, exchange information and expenditures, and work together using the Internet, often without knowing each other beforehand. And all deals they make depend on the reputation they have built up via reviews and the products and companies they choose to support. Carpooling services mediate the trust between a person with a car and his or her potential passengers via recommendations from other former passengers. On private home rental platforms you rent a vacation home from a total stranger. Trust is mediated by these services, which have built systems that allow the user to, for example, verify the landlord's descriptions by reading other people's reviews, to guarantee his/her deposit and, in turn, for the landlord to check the renter's ID. Trust is the business model of the sharing economy. As Airbnb's slogan says, '2 million listings. 60 million guests. 191+ countries. Trust is what makes it work.'

51. The Capital of the New Economy is Trust, Rachel Botsman, TEDGlobal, 2012.

TRUST IS ACHIEVED IN VARIOUS WAYS

For consumers, trust is about expectations; more precisely, it's about something or someone living up to your expectations. Your expectations as a consumer in digital space, in turn, are defined by various factors. It could be everything from the design of a website that creates certain associations, personal experiences or things you've heard through the grapevine. Trust can also be achieved through different types of seals and certifications, where independent third parties ensure that what a company does can be trusted.

Some companies have built up consumer trust for many years in the physical world, which they bring with them into the digital universe.

> **COOP.** One of the largest food retailers in Denmark, COOP, has over 1.5 million loyal customers (in a national population of 5.6 million). The COOP Group uses personal data to personalise offers, analyse customer behaviour, optimise stores and provide members with deals from corporate business partners. But COOP, which is owned by its members, has set a limit to its data use. For example, the company has chosen thus far not to leverage customers' geographical data to push location-driven deals through to their smart phones. And COOP does not use price differentiation, that is, they do not set different prices based on knowledge of customer needs and behaviour. Customers get different offers depending on their shopping patterns.[52]

52. COOP interviewed August 2015 and March 2016.

MADE IN EUROPE

The economic effect of Snowden's revelations cannot be mistaken in Europe. They resulted mainly in distrust towards US-based companies. As the at that time Vice President for the EU Commission, Neelie Kroos, explained a month after the revelations:

"If businesses or governments think they might be spied on, they will have less reason to trust the cloud, and it will be cloud providers who ultimately miss out. Why would you pay someone else to hold your commercial or other secrets, if you suspect or know they are being shared against your wishes? Front or back door – it doesn't matter – any smart person doesn't want the information shared at all. Customers will act rationally, and providers will miss out on a great opportunity...If European cloud customers cannot trust the United States government or their assurances, then maybe they won't trust US cloud providers either. That is my guess. And if I am right then there are multi-billion euro consequences for American companies."[53]

The non-profit think tank Information Technology and Innovation Foundation (ITIF) concluded that the robust competitiveness the US tech industry exhibited before Snowden, has fallen victim to the US government's surveillance programmes and that the price tag actually exceeds the 35 billion dollars in lost revenue that they originally predicted would be the loss over three years.[54]

In 2014, SURFnet, the Netherlands' network organisation for higher education and research, decided to create an entire department to develop its own cloud services (such as SURFdrive). Erik Huizer[55], the CTO at SURFnet, said that this happened because universities discovered their data was on servers they didn't trust. At first they talked

53. Statement by Vice President Neelie Kroes on the consequences of living in an age of total information, memo, 4th of July, 2013.

54. Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness, Daniel Castro, Alan McQuinn, ITIF, 2015.

55. CTO Erik Huizer, November, 2015, personal interview.

about using servers in Germany or from another Dutch company, but then what would happen if these providers were at some point acquired by Amazon or Google? By developing their own cloud services they could be completely sure that the data would remain under their direct control and Dutch legislation. On the topic, Huizer stated: "Cloud servers are one of the first things where you can turn strict privacy laws into an advantage. Store your data in my country and we guarantee that it will be protected by our laws."

As testimony to this, many European institutions and companies do not want their data in the hands of US-based companies due to concerns about American surveillance and industrial espionage.

> **F-Secure.** "We never share your data with other sites or companies." This was the promise to customers that the Finish cloud company F Secure included when they launched their services in 2013, attracting one million customers in their first 9 months of existence. F-Secure also explicitly makes the point to their customers that all their data is physically stored in Finland.

Though American cloud companies are still dominant, non-US cloud services are beginning to get a foothold. Their selling point is a very specific trust relationship between them and their customers: 'Here, you are free from NSA Surveillance.' The message clear; a business outside US jurisdiction does not run the same risks of NSA listening in.

> **Qwant**. The French search engine has wedged itself into the distrust surrounding US-based online services. In 2014 it sold twenty percent of its shares to the German publisher Axel Springer to buy European servers. At the beginning of 2015, Qwant launched the child-friendly search engine, Qwant Junior. Although the search giant Google has announced similar plans, the French Ministry of Education said that it will use Qwant Junior in some French schools.[56]

56. Qwant Wants to be an Alternative to Google, New York Times Bits, 2014.

T-Systems. In November 2015, Microsoft, as one of the first major American cloud services, made a Europe-based solution available to its European customers.[57] Microsoft formed a partnership with Deutsche Telekom's subsidiary T-Systems as a so-called data trustee, which means that customers can use the Microsoft cloud in Germany under the custody of a company with German headquarters, and thereby subject to German data protection laws.

Although they have investors and offices in the US and Canada, the company behind Blackphone, the first privacy branded smartphone, has chosen to locate its headquarters in Europe – in Switzerland, a country that enshrined the right to private communication and email in its constitution, making it no longer just the country of bank secrecy but also a privacy hotbed. A company's location has become one of the ways to gain consumers' trust and, increasingly, that of governmental and enterprise partners.

Xapo. In January 2015, the Palo Alto-based company Xapo moved its servers to Switzerland. Xapo, which provides security and bitcoin services, got the sense from its customers that this wasn't enough, as the company's head office was still in the United States. So, at the end of the year the business moved headquarters from California to Switzerland.[58]

Zettabox. When the small American cloud service provider Zettabox established not only its servers, but also its headquarters in Europe in 2015, they did so with a direct reference to the forthcoming EU data protection legislation

57. Microsoft Announces Plans to Offer Cloud Services from German Datacenters, Microsoft News, 2015.

58. Switzerland is a banking capital. But a Bitcoin Capital, Fortune, 2015.

reform. In this way, they leveraged European data protection standards to stand out from other US-based competitors on the market.[59]

PRIVACY BRANDING

Many companies have determined that it's a good idea to market products based on privacy features and the company's privacy sensitivity. Many are doing so by differentiating themselves from multinational, data-driven tech companies. In particular, Apple has developed its 'privacy brand' by going to battle with the US government, issuing public statements against the data-driven business model and launching privacy features in products. Also Mozilla has made an effort out of presenting privacy as part of their company value system. For instance it is one of the 10 principles of the Mozilla Manifesto. A rising number of other companies are following suit.

KiDMEMO. The Finnish service KiDMEMO gives parents a platform to share photos of their children privately – and print picture books for a fee. The owners say they created KiDMEMO because they couldn't find an existing service where they kept ownership of their photos and could also keep them safe. 'Our service guarantees your online privacy' states their website, which also emphasises that pictures on the website can only be seen by you or the people whom you have shared them with.[60]

Cozy. The French personal cloud service provider Cozy.io, which also sells other digital services, is proactively marketing the company as anti-Google. In the beginning, the slogan read:

59. Cloud startup Zettabox touts privacy and local storage to appeal to EU customers, PC World, 2015.

60. CEO and founder Jenni Lahti, personal interview 2014 and September 2016.

'We cannot do evil' clearly a reference to Google's former 'Do No Evil' slogan. It was subsequently changed to: 'Ungoogle your digital life. Reclaim your privacy from Google.'

Startmail.com. The Dutch search engine startpage.com is free because their email service isn't. Startmail markets itself as follows: "Take Back Your Email Privacy. “Free” email services aren’t free – you pay for them by sharing the most intimate details of your life with corporations and marketers. With StartMail, your email is for only you to read. We make it easy for you to protect yourself from unwanted intrusion and mass surveillance."

Soverin.net is Startmails' competitor, also Dutch. It's even more direct in its marketing against the data-driven business model: "Just imagine…the postman opening your personal letters, the carrier listening in on your calls, the bank analysing your transactions. This happens to your ‘free’ email every day. Your personal messages are monitored and the data is sold for advertising...Soverin is the honest email service that doesn’t sell your data."

Some multinational companies use similar campaign tactics to show that they approach their customers' privacy differently than their competitors. Microsoft once had a campaign against Google.

Microsoft. In 2012, Microsoft led a fierce campaign against Google. When it emerged that Google's Gmail tracked all the content in emails to display personalised advertising, Microsoft's Hotmail promised not to and opened the site Scroogled.com to make fun of Google's personal data collection methods. They even made a cup emblazoned with 'Keep Calm While We Steal Your Data' and the Google logo. The site was shut down in

2013[61] and has since been replaced with whymicrosoft.com, where Microsoft, in a more moderate tone, compares its services with those of Google, Amazon, Cisco and Salesforce. More recently, however, Microsoft has backtracked in relation to its privacy promises and battle against Google.

61. Microsoft Shuts Down Scroogled Website, Business Insider, 2015.

Failing to deliver on a promise of privacy is more fatal than not making any promises at all.

CHAPTER 5

PRIVACY CHARLATANS

Apple's top boss Tim Cook is anything but timid. In mid-2015, as the keynote speaker at a dinner in Washington DC, he scolded his competitors. "Our privacy is being attacked on multiple fronts", he proclaimed. "I'm speaking to you from Silicon Valley, where some of the most prominent and successful companies have built their businesses by lulling their customers into complacency about their personal information. They're gobbling up everything they can learn about you and trying to monetise it. We think that's wrong. And it's not the kind of company that Apple wants to be."[62]

Cook's words were clearly directed at Google, Facebook and other companies with data-driven business models which provide 'free' services, those where customers pay with their data – without knowing the price. Only a small portion of Apple's revenue comes from advertising, but it's no secret that its products also collect data, both behavioural and health related. Tim Cook's words may very well be judged as hollow someday, but there's a good argument behind his promise. The company's business model, according to him, is based on the sale of physical products, hardware, and not the capitalisation of personal data. Apple also seems to focus on privacy within the organisation, where it's said that a team of experts is involved in all pro-

62. Tim Cook: Silicon Valley's most successful companies are selling you out, The Verge, 2015.

cesses, with direct access to Mr. Cook.[63] In 2016, Apple presented its work on 'differential privacy' to the public.[64] In general, the company has put itself forward as a privacy defender, even in regards to governmental access to their products, a role which they were quick to prove: that same year, Apple denied the FBI's request to crack its own security features to access data on a terrorist's iPhone.

If Apple one day decides to change its business model and concentrate all profit on its customers' data, or if it comes out that it in some way has bowed to state pressure, it will most likely be heavily judged by the public as a Privacy Charlatan.[65]

A Privacy Charlatan is a company that promises its customers a certain degree of privacy and data protection which it cannot actually deliver due to its technology, business model or policy.

A Privacy Charlatan may also be a company which, because of new requirements from authorities, social challenges, technical problems and decisions about the business, can no longer keep its privacy promises and fails to act on these new challenges in a timely manner.

No matter how well-intentioned, all promises of customer privacy may come up against some obstacles. But the real issue is whether or not the business addresses these issues with due diligence. For example, following the Snowden revelations in 2013, email service providers Lavabit and Silent Circle decided to shutter their operations as they realised they no longer could keep the promises they made to their users about privacy and anonymity.

Most tech companies today make pledges of varying degrees to their users beyond the site's basic privacy policy, in order to offer dif-

63. Apple 'Privacy Czars' Grapple with Internal Conflicts over User Data", Reuters, 2016.

64. Apple's New Privacy Technology May Pressure Competitors to Better Protect Our Data, MIT Technology Review, 2016.

65. Charlatans the new Wave of Privacy Profiteers, Zdnet, 2014.

ferent types of user control over data, e.g. in the form of fine-tuned privacy settings etc. These promises have been part of a necessary strategy to build or rebuild consumers' digital trust. But many enterprises are also beginning to realise that privacy and data ethics are actual selling points as well, and we'll surely see more and more of them presenting user privacy and ethical data handling in their marketing strategies. But for some, that will be all it is: a marketing strategy. Not everyone will actually have the business practices to support the promises made in the marketing campaign and, most importantly, not all will show due diligence to their users when new conditions or requirements crop up.

Promising privacy to customers with the knowledge that these pledges can't be kept is worse than not mentioning privacy at all; it simply creates too high of an expectation. When you use Twitter, for example, you are well aware that your tweets are public, and most Twitter users will act accordingly. Breaking a privacy promise with users is a breach of trust and will comport fatal consequences both for customer privacy and for the brand.

Ashley Madison. As a website that facilitates infidelity, Ashley Madison promised to delete user data for paying customers. But it didn't quite delete all the data. In 2015, the site got into big trouble when hackers stole their database on 37 million customers and threatened to publish sensitive information – including the sexual fantasies and names of well-known people. The hackers demanded that the Canadian firm behind Ashley Madison close the site down permanently. Ashley Madison chose not to listen and the data was doxed online to disastrous consequences – one man even committed suicide. A key issue with Ashley Madison's approach to privacy, according to an investigation conducted by the Canadian and Australian Privacy Commissioners, was that there were a number of trust marks on the website which gave the impression that the site adhered to high privacy and confidentiality standards. The

investigation underlined that this may have been material to users' decisions whether or not to use the site.[66] In the wake of the breach, the company is still trying to survive as a new, more general dating service.[67]

Anonabox. In 2014, one specific privacy project received an extraordinary amount of attention on the crowdfunding platform Kickstarter. A large amount of capital was raised for the new super tool Anonabox, a Tor-based router that would provide users with complete anonymity in everything they do online. After having collected over $600,000 in two days, the project was stopped abruptly and the money was frozen. Experts had reviewed the solution and pointed to a number of security vulnerabilities. They also found a striking resemblance between the product's images and photos of a Chinese router which was already freely available on the market.

Spotify. In August 2015, the Swedish music streaming service Spotify changed its privacy policy. Wired Magazine looked into the change and revealed that Spotify would henceforth have access to all the photos, contacts and the location of your phone, even for paying subscribers.[68] This caused an uproar on Twitter. Why did a music service need people's photos? The inventor of Minecraft, Markus Persson, sent a message to his 2.5 million plus Twitter followers: Do No Evil Spotify. Subsequently Spotify CEO Daniel Ek apologised and made a privacy promise that the sharing of this data would be voluntary.

---

66. Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner, 2016.
67. Ashley Madison Faces F.T.C. Inquiry Amid Rebranding, New York Times, 2016.
68. You Can't do Squat about Spotifys Eerie New Privacy Policy, Wired, 2015.

Tinder. The popular dating app Tinder has an extensive privacy policy, where it makes numerous promises to its users. But this is easier said than done. In April 2016, Swipebuster.com went after Tinder and told its users that for a small payment they could find out if their boss, girlfriend or others use Tinder. They would do so not by hacking Tinder, not by scraping data, but by searching the databases that Tinder's official API makes available to third-party developers. Swipebuster didn't actually want to expose infidelity. Rather the developers behind the site said they wanted to point out that the issue is not just people oversharing, but that companies don't inform users when their data is available to others.

SOCIAL PRIVACY

"Facebook's current privacy model revolves around networks", Mark Zuckerberg wrote in an open letter in 2009. He continued to explain a new type of control Facebook users would have over the content they share with family and friends moving forward. "The plan we've come up with is to remove regional networks completely and create a simpler model for privacy control where you can set content to be available to only your friends, friends of your friends, or everyone."[69]

Facebook. Facebook introduced 'privacy settings' to social media. It gave many users the feeling of having privacy, as long as they had the correct settings, but it's important to remember that Facebook's privacy model is actually about 'social privacy'. The fact that you can create boundaries around your content so groups of users in your network cannot see it, does not mean that Facebook and their paying third-party partners are also locked out. Anyone who has tried stalking a non-Facebook friend with graph.tips knows that a person's likes, comments and

69. An Open Letter from Facebook Founder Mark Zuckerberg, Facebook, 2009.

tags are public-by-default. In addition, the settings are difficult to understand, and change so often, that many users can't keep up. Facebook has also promoted itself as a privacy campaigner by offering access via the TOR network. This might change your location just like when using a VPN, but once you post something on Facebook, you are identified by Facebook. Despite this, in June 2016, Facebook went as far as calling itself a 'privacy-enhancing' platform.

The concept of 'social privacy' is also the point of departure for what is known as 'ephemeral' apps and software. With these, users can send messages and images that self-destruct after receipt. Slingshot, Poke and Gryphn have very few members, but everyone knows Snapchat, one of the first apps to address internet users' growing need to gain control over their online communication and the context they share it in. Snapchat has more than 150 million active users according to their own statistics.

Snapchat. Snapchat's core user group is 13- to 34-year-olds. Through Snapchat, you can send photos or videos that disappear a few seconds after the recipient sees them. The service is often used for silly, harmless snaps, but it's also used to send more sensitive pictures. It simply feels more private when you are promised that the picture will disappear after receipt. But Snapchat is not actually private. There are services that make it possible for the recipient to save images when they receive them, and in 2014 at least one of these services was hacked, causing 200,000 snaps to be leaked on the web. The American Federal Trade Commission (FTC) criticised Snapchat for misleading users, as the app also collects much more data than promised, seriously damaging the service's reputation. Interestingly enough, although Snapchat is constantly being watched by authorities, the company has been successful with its message that content is in fact deleted.

Snapchat's success is proof that users of social media services have a need for control over their data. But Snapchat's self-destroying user content, as well as most social media privacy settings today, address this need only. With apps like Snapchat and refined privacy settings, you get a sense of 'social privacy' – that is, a degree of control over your social identity that may vary in different social contexts and networks, such as friends, family and professional relations. But this does not imply that you are also protected from corporate and state surveillance.

WHICH IS WHICH?

There's always a risk that the core of a company's approach to online consumer privacy will be affected by new business requirements, such as may happen in the wake of an acquisition. At the same time, a company's data ethics policy is a result of many interests. Not one element will show the true colours of a company's moral compass when it comes to the treatment of its customers' data, but the sum of all can guide customers, media, experts and investors when deciding which company's privacy promises to trust and which ones to reject as Privacy Charlatans.

WhatsApp. In August 2016, WhatsApp, one of the world's most used chat apps, announced it would begin sharing users' private information (such as their phone number and data analytics) with Facebook and is preparing to allow businesses to message users.[70] When the service's Ukrainian founders sold WhatsApp to Facebook in 2014, some users left the service in favour of other messenger services, Telegram in particular. The concern was whether or not WhatsApp could be trusted not to compromise one's privacy by selling targeted advertising (which the founder originally said they wouldn't do), as it was now

70. WhatsApp to give users' phone numbers to Facebook for targeted ads, The Guardian, 2016.

owned by a company thriving on personal data. WhatsApp used to cost one dollar a year to use, but in early 2016 it became yet another 'free' service.[71] The founder talked about charging a fee from corporate customers in the future, but WhatsApp's exact business model was, at least in early 2016, still an enigma.[72] In the wake of Apple's battle with the FBI, WhatsApp decided to implement end-to-end message encryption[73], a move celebrated by many as a victory for global user privacy. But at the same time, concern was raised by sceptics. WhatsApp, they said, was still asking for access to a range of information on mobile devices, including contacts and metadata, and it was not clear from its privacy policy what data the app uses. When WhatsApp presented its new data sharing agreement with Facebook in Auguts 2016, the same sceptics' ongoing concern about WhatsApps' relation to its parent company, and its commercial interests in the service was confirmed.

MORE (PERCEIVED) SECURITY, MORE SHARING

Carnegie Mellon professor Alessandro Acquisti has published several studies together with other prominent researchers illustrating the way in which people are enticed to share their data. One of the conclusions is that the more privacy and the more control users think they have over their data on a website, the more they dare to share about themselves – including intimate details.[74] In his research, Acquisti has also documented how companies which are transparent about their use of data need to live up to the privacy promises they make, as transparency in itself can actually make users suspicious. Finally, he also

71. Facebook's WhatsApp Is Now Free, Recode, 2016.

72. Whatsapp is nearing a billion users Now It's Time to Find the Money, Wired, 2016.

73. Forget Apple Vs FBI, Whatsapp just switched on encryption for a billion people", Wired, 2016.

74. Misplaced Confidences: Privacy and the Control Paradox, Laura Brandimarte, Alessandro Acquisti, George Loewenstein, WEIS, 2010.

proved that businesses who generally entice trust among their customers can do much more with personal data than others who do not have the same level of user trust.

Many people believe that the simple existence of a privacy policy means you can trust the company to treat personal data properly. Richards and Harzog have similarly argued that big data companies should "...vow to be Protective, Discreet, Honest, and above all, Loyal to data subjects". If they are, people will put more trust in the concept of big data in general, and they will disclose more and provide more accurate information in safe, sustainable ways.[75]

75. Trusting Big Data Research, Neil M. Richards and Woodrow Hartzog, Stanford Technology Law Review, 2016.

A new market for privacy-enhancing products and services is emerging. Not unlike environmental technologies, we'll see an increase in demand for privacy tech.

CHAPTER 6

A NEW MARKET FOR PRIVACY TECH

While data ethics has become part of the agenda at some visionary companies, a whole new market has emerged for products with privacy and personal control as their main selling point. These privacy tech products often depart from and further develop well-established PETs, Privacy Enhancing Technologies. Privacy enhancing chat and messenger services, smart phones, email, file sharing and data storage services, personal local cloud devices, search engines without tracking, cookie blocking, VPN clients and so on. These are products and services which include mobiles and tablets from the infamous Blackphone, search engines like StartPage, DuckDuckGo, Findx, Qwant and Hulbee, chat apps like Threema, Signal, Wire and Wickr, secure phone services like RedPhone, secure browsers like PrivaFox, Brave, Firefox and TOR, and a wealth of VPNs (Disconnect.me, Hotspot Shield and F-Secure). Often these new services and products are fiercely discussed, particularly by tech experts and tech media who assess the minute details of security, data protection features, the technical solution's degree of user anonymity as well as the organisation and business model behind it.

The emerging privacy tech market is an important trend shaping the data ethics paradigm shift. These products can be seen as a direct response to consumer demand to protect privacy, a reaction to the

stories of major surveillance and data leaks. They are different from the more traditional anonymisation services in that they combine user friendliness with data protection and privacy controls. They often have the clearly-stated goal of creating 'privacy for the people' and not just for the few tech-savvy elite.

DuckDuckGo. Search engine DuckDuckGo's slogan is: "Switch to the search engine that doesn't track you." Founded in 2006 as an alternative to Google, it was built on the core value of integrity as it relates to privacy and anonymity. It doesn't store users' IP addresses or send unique cookies to track users' searches per default, and it redirects traffic between DuckDuckGo and the links users click on so other websites can't track individual searches. Gabriel Weinberg founded DuckDuckGo based on two principles: one was to break with the 'filter bubble' – the Google model where search results are selected based on a user's previous searches, location, shopping patterns and interests. The second was about privacy, which has proven to be the core principle upon which DuckDuckGo built its brand.[76]

PrivaCore. The PrivaControl browser add-on, the PrivaFox browser, and the Findx.com search engine: these three privacy products are all backed by Danish start-up PrivaCore Aps. Brian Schildt explains that he got together with Brian Rasmussen to develop the products for two reasons: their children needed alternatives to escape massive online surveillance and, at the same time, they intuited it would be a good business move to develop these products. Based on Canadian Privacy by Design principles, and due to the transparency of open source code and other PET-products like

76. Duckduckgo: The Plucky Upstart Taking on Google with Secure Searches, The Guardian, 2014.

Open Street Map, PrivaCore services are, at least for now, available free of charge. Like DuckDuckGo, PrivaCore is determined to make money on context-based advertising (as Google did in the beginning, before it decided to bet on personalised marketing). They also believe there's a market for un-tracked paid search activities.[77]

Silent Circle. Silent Circle was established in 2011 by Internet pioneers Mike Janke and Phil Zimmerman. In 2013, Silent Circle consisted of the services Silent Phone, Silent Text and Silent Mail, which are based on end-to-end encryption, meaning that communication can only be read by the sender and receiver and not the provider of the communications service. When Snowden's revelations rolled through the media, Silent Circle, based in the United States, came to the conclusion that they could not keep their users' email communications safe from the NSA. Hence they decided, like the encrypted mail service Lavabit, to close their email service down immediately: "We have not received subpoenas, warrants, security letters, or anything else by any government, and this is why we are acting now", they explained.[78]

Blackphone. In 2014, Silent Circle moved its headquarters to Switzerland and launched the world's first privacy smartphone, Blackphone, in cooperation with Spanish Geeksphone. Designed with privacy as the default, the mobile device runs on an Android operating system designed in-house, PrivatOS, and has a set of applications for secure, encrypted communication. The original target group was the general consumer, today it's mainly businesses. The first version of Blackphone sold far

77. Co-founder Brian Schildt, August 2016, personal interview.

78. Two Encrypted Email Services Shut Down to Avoid NSA Snooping, MashableUK, 2013.

below expectations[79], and it's uncertain how it's going with the following version, based on Android as operating system.

Puri.sm. "Purism is devoted to providing the highest quality hardware available, ensuring the rights of security, privacy and freedom for all users."[80] So promises the San Francisco-based company behind the Privacy by Design Librem laptops, which feature so-called kill switches so you can quickly turn off the camera and microphone.

Signal and **Open Whisper Systems**. In November 2015 Edward Snowden tweeted about his daily use of Signal: an end-to-end encrypted messenger service produced by Open Whisper Systems. He was on the front page of the Open Whisper Systems website alongside a number of other privacy and security experts urging everyone to use the organisation's services in general. Open Whisper Systems is both a large community of volunteer open source contributors, as well as a small non-profit with a team of dedicated grant-funded developers. Its aim is to develop secure services that are easy to use, for everyone.

USER FRIENDLINESS

Services that anonymise and secure users' communications against surveillance have been an integral part of the Internet's history. While PET-products first and foremost were something for the tech nerd or activist, many of the new privacy products are increasingly focused on being user friendly. There is in fact a rising demand for these types of products from everyday consumers and businesses, as demonstrated by their sales and user statistics.

79. We Know People Care about Privacy so Why Don't They Pay for it?, The Guardian, 2016.
80. About, puri.sm, 2016.

Practically all new privacy products recognise that although consumers have an inherent need for privacy in some form or another, they are also too comfortable to make any extra effort to get it. But if the consumer had a choice between two equally user-friendly services where one of them offered greater privacy and control, the consumer would choose the latter (as Aquisti has shown, Chap. 3). Convenience is the mantra – not everyone has technical skills. If we want to create secure products for the public, privacy protection and control features need to be seamless and user-friendly.

Wire. There are more and more chat and messenger services built upon the idea of private communication, only accessible to those who opt for built-in end-to-end encryption and a strict resistance to profiling and targeted advertising. For example, there's Threema, Wickr and Signal. Then there's the Swiss service Wire, which is taking an extra step and letting you 'skype', that is video chat, with end-to-end encryption. One of the original Skype inventors, Janus Friis, supports Wire and a number of former Skype engineers are working on the service also. Wire has a strong focus on being user friendly.

User friendliness – or lack thereof – was one of the major challenges for the first version of the Blackphone and as a result it flopped in sales. One cause was most likely a number of organisational challenges and changes in the company's management. But we cannot discount the fact that it had developed its own operating system, PrivateOS, which wasn't quite user friendly and had a very limited range of apps. At the same time, Blackphone and other secure products were challenged by broader-reaching, more general developers (such as Apple) marketing their own privacy features. That, for most consumers, was enough in itself.

PRIVACY PRODUCTS ARE NOT NEW

Products, machines, inventions and technologies designed to protect our privacy are not new phenomena. Historically, challenges to privacy have served as inspiration for inventions that can protect different aspects of our privacy. Ideas about privacy have therefore often been a driving force for new companies, markets and products.

In the beginning of the last century, the 'bathing machine' was invented in the UK. The bathing machine was in essence a privacy product designed to protect its users from the gaze of others. At the time, it was not reputable to appear in public in your swimsuit, especially not for women, but it was also widely believed that seawater was healthy and even a cure for some diseases. The bathing machine was thus designed to shield women (in particular) who were taking a dip in the sea from the prying eyes of those along the shore. A large wagon was pulled in and out of the water by a horse, on rails or by means of cables that were powered by a steam engine. One could then descend into the water without being leered at from the beach. The bathing machine was a well thought-out invention with various built-in privacy features, such as a canvas tent that would be lowered from the sea-facing door to give the bather even greater privacy. At some beaches, staff was even hired, the so-called 'dippers', strong women or men who could help the user in and out of the bathing machine.[81]

Another example of an early, innovative privacy product was the Hush-a-Phone. In the early phone age, this accessory was invented and marketed in the US under the slogan 'Safeguarding privacy – so others can't hear confidential matters". Hush-a-Phone was a cup-shaped tube that you could mount on any handset to make it difficult for others to listen in on your conversations. At the time, telephones in America were not owned by consumers, but by AT&T, which happened to have a monopoly over the market. AT&T took Hush-a-

81. A social history 1750-1914, Walton, John K. The English Seaside Resort, Leicester University Press, 1983.

Phone to court as they believed that they had the right to prohibit telephone accessories which they didn't produce themselves. Ultimately Hush-a-Phone won their right to existence and paved the way for a new market of secondary phone accessories.[82]

ANONYMITY TECH

In the Internet age we have moved on from early computer cryptography to more varied forms of privacy protection that provide users with multiple degrees of control over their personal data and also offer them anonymity online. The concept of Privacy Enhancing Technologies (PET) was originally introduced as a category of technologies and services that first and foremost anonymise internet use and communication.

TOR. One of the most talked about and used anonymity services is TOR, a freely available software that hides the user's location and internet usage by routing Internet traffic through a network of servers hosted by volunteers around the world. TOR was originally developed in the 1990s to protect US intelligence services' communications. In 2004, it was released under a free license, then in 2006, the Tor Project Foundation was established as a non-profit organisation to maintain TOR. With its long history as one of the safest and best anonymisation tools, TOR has become the symbol of PET-services online, and thus one of the key tools for activists and journalists.

PGP. Another, more traditional PET-service is PGP (Pretty Good Privacy). PGP was developed in 1991 by one of the key people behind Silent Circle, Phil Zimmermann, as a tool to protect political activists like him. It is a hard-to-use encryption tool that is used to sign, encrypt and decrypt texts, emails, files

82. Hush-A-Phone v. United States, 238 F.2d 266 (D.C. Cir. 1956).

and folders. For many years, PGP was managed by the PGP Corporation with offices scattered around the globe. Symantec acquired PGP in 2010.

PRIVACY IS A COMMITMENT

There are big variations in the products and services that claim security and protection of their users' privacy. At a time when privacy has become the new black, there's a battle going on about the definition of what privacy is and how it's best protected.

To promise privacy is to make a commitment which requires continuous work and focus. Often, the original intentions were honourable, but problems arise when a business only sees its handling of user data and privacy as good business and not as a core ethical choice. Snapchat, for example, was founded upon the idea that Internet users want but lack control over their digital social lives. It turned out to be a great business idea, and one of the most profitable. But if we hold Snapchat up as an experiment, a new model for user control and privacy on the Internet, the company has failed. News stories about data leaks and accusations from the US Federal Trade Commission are evidence of this, sure to leave a mark on consumer trust in the future. In fact, the worst thing a company can do is to promise a level of data protection and control which, in the end, is nothing more than lip service. Users will see it as a breach of trust, and business ideas regarding privacy and user control are nothing without the trust of consumers.

We can choose to view privacy as an obstacle, or we can choose to see it as a natural part of innovation.

CHAPTER 7

PRIVACY EMBEDDED IN INNOVATION

"We're concerned that the EC's proposed data protection reforms will put European businesses at a competitive disadvantage in a global market, by placing restrictive controls and high cost-burdens on innovation and investment." Such were the words from Mathew Fell, Director for Competitive Markets at the UK's primary industry lobby organisation, the CBI.[83]

Fell's statement, made in 2012 just after the European Commission released its first communication on a comprehensive revision of the existing European data protection regulatory framework, shows he was particularly worried about the reform's impact on data-driven innovation. He was not alone in his alarm over European competitiveness, and a chorus of voices from the Internet industry chimed in with similar opinions. Although the EU Commission described the reform as a way to support the European common market and the free movement of data, it also used the word 'protection' over 100 times in its

83. CBI Claims EU Protection Laws Stiffle Innovation, Computing, 2012.

first proposal for a reform.[84] It was a thorn in the eye of an industry built on the movement of data.

The words we use to talk about data and innovation define legislation, policies and business processes. They're not just words, but descriptions that guide and direct actions. The idea that data protection is a limitation to innovation has been a recurring theme not only in political debate, but in a more general digital business context. Data protection is seen as a limit to creative, innovative digital enterprise development, an additional, cumbersome legal hoop to jump through, unrelated to the needs of consumers or of digital progress in general. This is may be caused by an assumption that, when we talk about digital innovation, we're primarily referring to innovative ways of collecting, analysing and categorising data, sharing it, or streamlining and personalising services based on it. Data protection and privacy are then essentially stop signs on the creative process highway. The obstacle you must overcome when new solutions are developed. For this reason, data protection is often only brought up at end of the innovation process, when the legal department gets involved.

Rather than being an afterthought or stopgap, privacy and data protection should become a prerequisite for business development and innovation.

The case with Pokemon GO, launched in July 2016, shows that privacy was an afterthought. Children are the primary users of the game, in which you catch Pokemons in the real world through your smartphone's camera by using virtual reality technology. Pokemon GO didn't put enough thought into gamers' privacy, which quickly led to sharp criticism from security and privacy experts and spurred politi-

84. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, European Commission, 25.1.2012.

cians and data protection authorities to demand answers regarding the company's use of that data.

SURVEILLANCE CAPITALISM

Harvard professor Shoshana Zuboff calls the data-driven business model the 'surveillance business model' and the underlying system 'surveillance capitalism'[85], and says it's been allowed to flourish because so far we've uncritically accepted the way industry giants stage the status quo in business development and innovation. As Internet users, we are asked to accept a natural order of things in which big data is the guiding star, users are 'unpaid labour' and our personal data is just 'exhaust' and of no value to us.[86] But nothing should be taken for granted, she argues, as we still have time to change this infrastructure into a more democratic model. She calls upon European institutions and citizens to challenge the existing business model and create an alternative future. "If the digital future is to be our home, then it is we who must make it so. Against the Surveillance Capitalism of Big Data", as she wrote in the German newspaper, *Frankfurter Allgemeine*.

DECLARATIONS OF INDEPENDENCE

We can choose to view and talk about our privacy as an obstacle, or we can choose to see it as a natural part of the innovative processes. A nascent tech and business movement is doing just that. With declarations, manifestos and public statements, they promise solutions and business models that protect data privacy. They describe alternatives to the web's dominant operating, built on non-transparent tracking of user data. It's not a natural fact that boundless and often covert surveillance of individuals is the only way to do things online. We should, they say, insist on a different digital future by telling an alternative

85. The Secrets of Surveillance Capitalism, Shoshana Zuboff, Frankfurter Allgemeine, 2016.
86. A Digital Declaration, Frankfurter Allgemeine, 2014.

digital story; we must talk about other ways of doing business. Virtually all of these new companies are built on a social mission.

> **Ind.ie**. The designers Aral Balkan and Laura Kalbag are developing ethically-designed services. Their stated mission is to create everyday things for everyday people based on socially responsible principles, which they define as 'decentralised, zero-knowledge, and private by default'. They've presented an idea for a device (Indie Phone) that does just that, and they've developed services such as Heartbeat, a peer-to-peer social networking client for Mac OS X, and a content blocker (or as they call it a 'tracker blocker'), Better, for the iPhone and iPad.

"We want to create a new topology of technologies grounded in individuals owning their own data", said Aral Balkan.[87] "The common misconception is that such systems are difficult to design and develop. They're not, but they do require a different business and funding model." Balkan believes that the Silicon Valley model funded by venture capital is the core of the problem. He also thinks there is a different way forward: "You won't get billion-dollar unicorns, but you can create sustainable, long-term enterprises that sell products to people instead of selling people as products. It is possible to build systems where individuals have ownership and control of their own data, on their own devices, instead holding it in a cloud where a corporation has ownership and control."

> **Jolla.** This Finnish company has designed and developed a smartphone and tablet that run on a proprietary operating system called Sailfish OS. The people behind it were originally employed by Nokia, where they developed the Linux-based operating system, Maemo. However, since Nokia decided to shut down the project and bet on Microsoft Windows' mobile platform, they left the company and established their own.

87. Aral Balkan, April, 2015, personal interview.

Jollas' slogan is just one word: 'UNLIKE', a reference to Facebook's 'like' button. With such a motto, Jolla is signalling that it's not like other tech companies. Jolla writes on their website: "We do not share your personal data with third parties without your express authorisation. We are not building a business on monetising your personal data. We can succeed as a business when our users are happy and know that they can trust us not to share their data with others if they have not authorised it expressly."[88]

MeWe. This social network states: "MeWe challenges the status quo by making privacy the foundation of online social experiences." MeWe has a 'Privacy Bill of Rights', that, among other things, promises not to track users, profile them or give third parties access to their data. They promote the service with the MeWe challenge: "Is your social network stalking you?" An online tool shows the user how many tracking cookies are being used by social networking services like Facebook, Instagram, Youtube, and LinkedIn. Their front page campaign film shows trendy young people doing various creative free time activities with the theme 'We are not for sale'[89]

ProtonMail. Declarations about privacy made by new enterprises are often recieved with enthusiasm among consumers. Mail provider ProtonMail's crowdfunding campaign was launched in 2014 as an anti-surveillance, pro-privacy product: "We believe that privacy is a fundamental human right that must be protected at any cost. The advent of the internet has now made all of us more vulnerable to mass surveillance than at any other point in human history. The disappearance of online privacy is a very dangerous trend as in many ways

88. Jolla.com, 2015.

89. mewe.com, 2016.

> privacy and freedom go hand in hand."[90]It was the most successful software product campaign in crowdfunding platform Indiegogo's history. ProtonMail's original campaign goal was $100,000, but by the third day they had doubled that amount. After one month, it had raised over half a million dollars.

Companies can and do in fact operate with privacy as innovation, articulate their business values around an individual's right to security and privacy, disassociate themselves from the data-driven business model, and explicitly describe their ideas for an alternative natural order in the digital business environment. They do so with slogans, manifestos and declarations most often located prominently and visibly on their websites. At the same time, a large portion of these businesses focuses on raising awareness. Several of them support or participate in campaigns in favour of privacy and data protection. Silent Circle's Phil Zimmermann and Mike Janke travel around the world to various tech conferences to present their view on digital privacy. Ind.ie's Aral Balkan is famous for his speeches on surveillance capitalism and design at events and conferences from the Big Brother Awards to the UN Internet Governance Forum.

ANTI-SURVEILLANCE SOCIAL REVOLUTIONARIES

One might deem such alternative tech companies to be a new category of technology revolutionaries. The original anonymity and privacy services were developed as tools for groups with the most exposure and risk: activists and critical journalists. Similarly, many privacy-enhancing services emerged in the wake of events which illustrated the democratic issues at stake in the digital era's dominant, data-driven business model. A whole series of anti-surveillance services and anonymisation tools were launched just after the NSA surveillance revelations of 2013. And Ello, for example, came into existence after it

90. indiegogo.com/projects/protonmail, 2016.

emerged that a group of drag queens who used their stage names on Facebook had their profiles shut down due to the social network's real name policy. Many of the missions presented by these alternative services are based on the idea of creating a fair balance of power between the individual and the institutions of society, the government, and data giants.

These tech revolutionaries describe privacy as the foundation for democracy, creativity and freedom of expression, and they see a chance for development where these values are threatened. It's a new type of company that generally doesn't measure its own success in common business lingo, such as market differentiation, profit and sales figures, but with terms from the world of socially conscious organisations.

Protonet. Hamburg-based Protonet's co-founder and CEO, Ali Jelveh, took the title of Chief Revolution Officer. It's a title he uses when he travels to talk about Protonet's main product: a platform for project management and collaboration in a secure, private cloud service. He describes his business as a social revolution that could change the way we think and act.

Diaspora. The non-profit social network Diaspora labels itself as anti-corporate. It's not owned by any person or entity and will never be taken over by a corporation. It states that your 'social life will never be sold to advertisers' and you won't have to 'conform to someone's arbitrary rules.' You can chose where your data is stored from various 'pods' hosted by different individuals and institutions.

Ello. One of the new social networks in 2014 was Ello, launched by a group of designers, artists and entrepreneurs. Already in a beta version, the network, according to its own data, had 3,000-4,000 sign-ups per hour and had to temporarily close down for more. They called themselves 'Anti-Facebook', a

moniker which lived on in the many media stories that followed Ello's launch. Reported stories described how people, tired of Facebook's targeted and intrusive advertising as well as their real name policy, streamed from Facebook to Ello, because the latter allows users to go by aliases and rejects the ad-based business model. Ello is built on a mission statement which among others reads: "...We believe a social network can be a tool for empowerment. Not a tool to deceive, coerce and manipulate – but a place to connect, create and celebrate life. You are not a product."[91]

PRIVACY BY DESIGN

We are beginning to see companies stand out by embedding privacy protection and features at the beginning of their design processes rather than waiting until the end. Their businesses are built upon 'Privacy by Design' – PbD principles. The first PbDs were developed in the 1990s by Ann Cavoukian, former Director of the Data Protection Agency in Canada.

Privacy by Design is the idea that the default setting of the service is private – private by default – and that it's designed and developed with privacy as a point of departure, not an afterthought.

The EU's General Data Protection Reform highlights PbD in Article 23, which also identifies a number of principles to ensure that public and private data processors implement technical and organisational measures to minimise personal data collection and handling. The concept of Privacy by Design can be used constructively, but since it has no universal definition, it can also be abused. One of the authors

91. ello.co, 2015.

of the ENISA report *Privacy and Data Protection by Design*,[92] Jaap-Henk Hoepman[93], describes how he has seen hard-core data-driven services that track their users across the board, call themselves PbD.[94] In the report, Jaap-Henk Hoepman, along with a number of other experts, describes Privacy by Design solutions that can and should be injected into digital business development. He and his colleagues point out that many basic data protection features and functions such as encryption are ignored when services are developed due to lack of awareness and knowledge among developers.[95]

A BUSINESS PHILOSOPHY

The Privacy by Design concept has been criticised for trying to solve a social problem with a technical solution, arguing that privacy cannot be guaranteed by technology alone. It's a good point, considering that the main focus so far has been on how to embed data protection in technology (of which there is also a great disagreement as to which solutions actually achieve PbD in the best possible manner). However, we can also look at PbD as a business philosophy, as an innovative approach where privacy is the starting point for the various inventive processes a company initiates – from design and technological development to human resources (e.g. employee training) and corporate marketing. In this way, Privacy by Design principles become a general guideline when building alternatives to the data-driven, public-by-default business model.

---

92. Privacy and Data Protection by Design – from policy to engineering, George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner, ENISA, 2014.

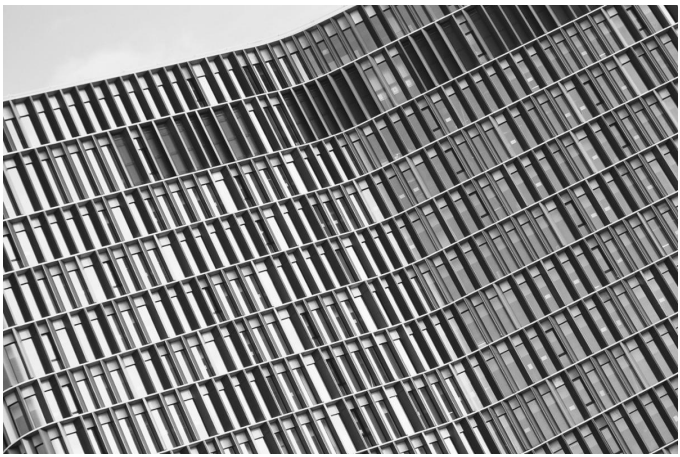
93. Jaap-Henk Hoepman, March, 2015, personal interview.

94. Privacy by Design: An idea whose time has come, Computing, 2015.

95. The Canadian Ryerson University's Privacy and Big Data Institute (where Ann Cavoukian is Executive Director) is currently developing a Privacy by Design certification system.

Vai Kai. For Matas Petrikas[96], CEO of German toy company Vai Kai, whose main product is a set of Internet-connected wooden dolls, customers privacy is the basis of all design and innovation decisions. "Privacy by Design, to me, means that we take the position of the privacy-aware and concerned customer, and we build a way for them to get what they want. The needs of this specific customer must be fulfilled and our product is designed to do excactly that", said Petrikas. For example, Vai Kai does not include a camera and microphone in their internet-connected dolls, which are private by default: "We think about privacy as a value all the time. It is part of our conversation. I assume other companies would never have had the conversation we had during our development phase that led to the conscious decision not to include a microphone," he said. The very idea of privacy is based on values that come from within: "You can represent something only if you are aware of it. If you are not aware of data privacy, it's not even part of your value system. We are an EU-company with our own unique view. The idea of privacy is part of our value system and it is also part of our customers' expectations." In particular, Petrikas sees his European customers' growing privacy awareness as a competitive advantage for his company.

96. CEO Matas Petrikas, March, 2016, personal interview.



An increasing number of investors are using privacy and data protection as criteria for funding.

CHAPTER 8

INVESTMENTS IN DATA ETHICAL BUSINESSES

Privacy and data ethics are starting to catch the eye of investors. IT and cyber security companies have long benefited from venture capital, and several former police and intelligence officers have established thriving consultancies which help other businesses and governments secure their commercial secrets and systems.

IT security and privacy go hand in hand, but the former has received more attention than the latter, and when New York investor Fred Wilson proclaimed in 2010 that there is money to be made on privacy, he was one of the first.[97] Since then, he's invested in DuckDuckGo and Bitcoin, and there are an increasing number of other investors who believe there's a market for Privacy Enhancing Technologies and data-ethical businesses. More and more innovative individuals and investment companies are declaring allegiance to privacy not only for social reasons but for economic ones. They see privacy as a good investment and it's therefore also part of the business story told when pitching to investors.

---

97. There's Money to be Made in "Premium Privacy" Says VC Fred Wilson, Readwrite, 2010.

> **TRUSTe.** The American company TRUSTe issues privacy certifications to companies that meet specific requirements in relation to personal data. Its certifications may assure consumers that a given company protects user information in accordance with specific standards, such COPPA (Child Online Privacy Protection Act) in the USA and the former US-EU Safe Harbour agreement. Since 2008, when they went from non-profit to for-profit, TRUSTe has received several rounds of capital from investors, including 15 million dollars from Accell Partners in The Silicon Valley. The logic behind their business is convincing: "TRUSTe is uniquely positioned to help businesses address the growing privacy concerns threatening to limit the adoption of new technologies, such as mobile, fast becoming the most common way for people to interact online."[98]

One can certainly question the specific products and solutions of companies which use privacy as a selling point to attract investors. In 2014, the US Federal Trade Commission brought a case against TRUSTe because the company failed to issue annual re-certifications to 1,000 of its customers. In cases which involve start-up capital, we might also question the sustainability of the basic corporate social values concerning privacy, especially when a company simultaneously must develop an exit strategy and therefore cannot guarantee the longevity of its principles. Accell Partners, for example, invests in all types of data-driven companies including Facebook and Dropbox, and out of the 209 investments they've made, they have 172 exits on record (according to TechCrunch's Crunchbase). We can only speculate as to what this has meant for the customer and user data held by the acquired businesses.

98. Privacy Firm TRUSTe Raises $15M in New Funding, AdWeek, 2012.

Yet what all of these companies have in common is that they use privacy and data ethics as selling points and thus have translated the concept of privacy into to capital.[99]

Digi.me. The British platform Digi.me that says it wants to give individuals control over their data is popular among investors. In June 2016, the company received 6.1 million dollars from a single backer to build out its platform.[100] Within it, the user can assemble his/her financial and health data and set his/her own sharing parameters, or even sell the data to other companies. Digi.me also provides new insight about users. With its user agreement, Digi.me's corporate customers can gain access to genuine, updated, detailed data. With clear privacy promises and reportedly more than 400,000 users in 140 countries, Digi.me is part of the personal data store trend (Chap. 12).

CognitiveLogic. This big data analytics service directly addresses the privacy implications of correlating data and analysis in the public and health sectors. CognitiveLogic has stated that it will develop a system which makes it possible to safely combine and analyse datasets from different institutions and businesses, all while maintaining individuals' privacy[101]. In 2016, CognitiveLogic received 3 million dollars from American venture capital investors.[102]

Privitar. Another big data analytics service, Privitar also addresses privacy challenges in a very direct manner. Their

99. TechCrunch has on a continous basis reported on cases where privacy focused services and products have received start up capital.

100. digi.me raises £4.2M ($6.1m) in Series A funding round, digi.me, 2016.

101. CognitiveLogic Raises 3 Million in Series Seed Funding, Cognitivelogic.com, 2016.

102. CognitiveLogic Raises $3M To Help Enterprises Pool Big Data While Keeping Privacy Intact, TechCrunch, 2016.

solution is targeted at the correlation and analysis of big data in the finacial sector. According to its own description, it's designed to collect information while simultaneously maintaining individuals' privacy. They describe their product as 'privacy-preserving data mining' and also describe privacy as a competitive parameter. The company received 1 million dollars in start-up capital in 2015.[103]

ZenMate. In 2014, the Berlin-based service ZenMate, which encrypts its users' browsing activity and hides their IP-addresses, was given 3.2 million dollars from large investor companies, including Axel Springer and T-Systems (owned by Deutsche Telekom). In addition, the EU is adding capital to the company, which has a free VPN service with servers in the United States, Germany, Romania and Hong Kong. If a user wants more destinations, s/he can opt to pay for the premium version.

Neura. The US-based platform for the Internet of Things (IoT) has promised to give users the ability to personalise their various devices without compromising their privacy. In 2016, Neura received 11 million dollars in start-up capital.[104]

Brave. A browser that blocks invasive adverts and monitoring, Brave has received 205 million dollars in venture capital so the company behind it can make it faster, more private and facilitate micro payments. Brave's founder and Director, Brendan Eich (the former Director of Mozilla) says: "With Brave, users can fight back and secure their data on their gadgets while simultaneously supporting the content they want

103. Big Data Privacy Start Up Raises Over 1 Million in Funding Round, Bobsguide, 2015.
104. Neura, A Privacy-Focused Platform For The Internet Of Things, Raises $11M Series A, TechCrunch, 2016.

with micropayments."[105]Brave builds upon the blockchain technology of Bitcoin, where you can pay automatically and anonymously in a new revenue-sharing model between users and content publishers.

INVESTOR STORYTIME

The concept of 'Investor Storytime' is used by the creator of the social bookmarking site Pinboard, Maciej Cegłowski, to describe the tale companies build around their products and services to convince their investors of future success. According to Ceglowski, who is also an outspoken critic, in the digital business world there's a very specific story you have to know and be able to tell to your investors: "Investor storytime is when someone pays you to tell them how rich they'll get when you finally put ads on your site."[106]

He gives several examples of new companies which have managed to convince venture capitalists of their service's unique ability to directly target advertising to users, thereby obtaining millions to fund their start-up. The story about user data partly explains early digital entrepreneurs' obsession with data, he explains. To stay true to what they promised their investors, they have been forced to constantly find new ways to make their advertising more invasive and omnipresent. "And that's the motor destroying our online privacy", said Ceglowski. "Investor storytime is why you'll see facial detection on store shelves and checkout counters. Investor storytime is why garbage cans in London are talking to your cell phone to find out who you are."

Despite all this, the tide is turning. The story of a company's customer data can no longer stand on its own to convince investors of a business' potential success. This requires additional effort which goes hand in hand with consumers' increasing demand for data security and privacy. When it emerged that the ad-free social network Ello had

105. Propel invests in bitcoin-based browser platform Brave Software, Finextra, 2016.

106. Lecture, Beyond Tellerrand web design conference i Dusseldorf, Idlewords, 2014.

received venture capital financing (Fresh Tracks Capital gave them $435,000), the company was, not surprisingly, criticised for being unable to live up to its promise to remain ad-free and protect users' data. Critics believed that the company would eventually be forced to sell out, to do an about-face on their fierce privacy statements, once investors began to demand a return on their investment. As a retort, Ello registered as a Public Benefit Corporation in the US, which according to Ello makes it legally impossible for their investors to require Ello to display advertisements or sell their users' data. At the same, time Ello raised $550,000 more in venture capital.[107] Whether Ello can actually keep its privacy promise remains to be seen, yet their narrative holds another interesting aspect. It suggests that the story a company tells about its data protection is gaining more and more of a foothold and even competing with the tale of user reach and innovation by harnessing user details.

RushFiles. The Danish cloud service RushFiles.com is promoted with the slogan: 'Your Business Data – Securely Shared – By a Trusted Provider.' The service experienced strong investor interest because of its focus on security. As Rushfiles-investor Martin Lumbye[108] explains: "We assessed that everyone will want to know where their data is. Most use Dropbox or Amazon, and therefore very few know where their data is located and the law they are subjected to today. It's not legal as a company to use such services because of a lack of security; you expose people to unnecessary risks because the NSA has access to the data." RushFiles' data is stored in Denmark – a decision which was made because, according to Lumbye CEO of North-East Venture it's the safest option, especially when it comes to very personal information.

---

107. Ello Raises $5.5 Million, Legally Files As Public Benefit Corp. Meaning No Ads Ever", TechCrunch, 2014.

108. Martin Lumbye, March, 2016, personal interview.

PRIVACY AS CSR CRITERIA

The 'Ranking Digital Rights' (RDR) index is the world's first CSR-based evaluation of how tech companies respectively handle their users' right to freedom of expression and privacy. RDR was launched in the second half of 2015, and all companies which have been examined and ranked have fallen short in several areas.

Rebecca MacKinnon[109], the driving force behind the initiative, describes how the number of global CSR rankings that assess a company's influence on society has increased since the 1980s. RDR started with a focus on various companies' impact on the environment and employee working conditions, and it has helped create transparency around the way in which specific business practices influence society. At the same time, it has been instrumental in terms of helping investors ask the right questions of any company they consider backing. It provides the knowledge they need on that company in order to ensure its due diligence, which needs to be part of a company's risk management and thus its overall risk assessment.

Over the years, human rights has become an important CSR focus, said MacKinnon. For tech companies in particular, the handling of user data and privacy has the greatest human rights impact, and their users' confidence in their ability to do so is crucial to their success and corporate reputation. Consequently, it has become a key topic that investors now ask about.

"Investors are increasingly looking at security breaches, but also consumer privacy with the scandals that have erupted around privacy and surveillance, as what they call, in that business, 'a material risk'. Companies need to prove that they are planning against it, mitigating it, because it affects the company's profitability and their share prices and everything else. Investors want to see evidence that companies are dealing with these things responsibly," explained MacKinnon.

---

109. Rebecca MacKinnon, November, 2015, personal interview.

Ranking Digital Rights showed that none of the companies surveyed clearly explain whether users can check what information the company collects and shares about them. A comparison between surveyed businesses also showed that half of them do not explain whether users can access the information the company has stored about them and that many do not give details on how long they keep user data.

"Surfacing these problems provides investors with hard facts and data that they can then ask the companies about," and in reference to the conversations she's had with investors and venture capitalists about this topic, she also noted:

"Increasingly, these investors are looking at privacy as part of their criteria."

According to MacKinnon, the investor analytics firms that research companies on behalf of their investors are also beginning to look for information on corporate privacy practices. So far, they've lacked the methods and tools to investigate these practices, but with new initiatives that expose the corporate handling of user data, they've now got the tools to investigate and impose relevant requirements.

INVESTORS ASK FOR PRIVACY PRACTICES

Investors have always used social investment strategies, including those which ensure their investments will have both a financial return as well as a positive impact on society. Environmental or employee rights are key, but investors are starting to insist on data security and consumer privacy as criteria to protect their investments, especially for new tech companies. They are the first to see that there are risks associated with the collection and analysis of personal data which could potentially have fatal consequences for a company's reputation and brand.

A new breed of 'social investors' is cropping up: companies or funds specialising in investments with a social purpose, e.g. those which are privately run or run by trade unions and church societies. They are, of

course, the first to present requirements as to a company's social and environmental impact, including that of human rights. Venture capitalists are also jumping on the bandwagon, investing in new companies (in exchange for shares in the companies) assessed according to their innovation or their ability to penetrate a new market. Key criteria for such investments are often built on the innovative and pioneering elements of the business. Within recent years, however, several venture capitalists have come out declaring their support for ethical, human-centred and privacy-preserving services and products. Elon Musk, the founder of Tesla, invested 70 million dollars in ethical artificial intelligence research (OpenAI), and eBay's founder, Pierre Omidyar, has provided 250 million dollars to the journalist who wrote the first Snowden articles in 2013 (Glen Greenwald's media venture First Look Media). Omidyar's investment firm, Omidyar Network, generally invests in privacy, for example, in Privacy International and other similar charities.

The way companies treat people's data is coming to the forefront in international policy-making and negotiations.

CHAPTER 9

DATA ON THE POLITICAL AGENDA

With the digitalisation of societies, individual privacy protection is increasingly receiving attention from policymakers. In the digital world, data moving across jurisdictions is often facilitated by commercial transactions between companies and their customers. Lawmakers, policymakers and intergovernmental institutions are therefore placed in a position where they must consider and act on the challenges that arise when regional and national laws collide to create legal grey areas. The way companies treat citizens' data, not to mention how governments gain access to and make use of it for surveillance purposes, is a key topic in political negotiations around the globe today.

DATA PROTECTION IN EUROPE

Data Protection is not mentioned in the European Convention on Human Rights of 1948, where Article 8 defines the right to respect for private and family life. Data protection was added, however, to a number of legal instruments developed alongside technological progress as a further interpretation of the right to privacy within the context of digitalisation. The Council of Europe's Convention 108 (from 1981) details an individual's right to the protection of personal data against breaches that may occur during its collection and analysis, and aims to regulate the transfer of data across borders. The European

Charter of Fundamental Rights, which became legally binding in 2009 with the Treaty of Lisbon, also contains the right to data protection in addition to the right to privacy.

In 1995, a European Data Protection Directive was adopted. This was replaced in 2016 with a General Data Protection Regulation which has a binding legal force throughout every EU Member State and includes a number of legal requirements for among others businesses.

DATA PROTECTION, 1995

The European Data Protection Directive was adopted in 1995 to protect personal data transferred across borders in Europe by public and private companies via new online technologies. Originally spurred by the realisation that an essentially 'borderless' Internet was about to become a reality, the idea was to create a common legal framework which made it possible to exchange and process personal data across frontiers in a way that was also respectful of an individual's right to privacy.

In the mid-1990s, companies were just beginning to see the Internet as a business opportunity. The first browser, Mosaic, was launched in 1993, making it possible for an increasing number of users to view images and text on the web. The Internet and new online technologies were primarily seen as a potential opportunity, which the smartest IT companies and investors funded. However, lawmakers were also beginning to face the first privacy challenges of a single European market supported by new information and communication technologies. The 1995 Directive, however, recognised an entirely new type of player. While the original right to privacy was mostly defined as protection against government interference, it became obvious that data collection and processing would increasingly be carried out by both public and private institutions. The directive thus addresses any "indi-

viduals, governments, businesses, agencies and other bodies" responsible for the processing of personal details.[110]

The 1995 Directive was mostly aimed at the European market, but the entire Internet 'market' went well beyond the Continent; it was global and included the transfer of data on European citizens to countries outside the EU. The regulation also therefore specified that data can only be transferred to and processed in countries with the same data protection standards as at home. The United States, for example, does not have the same standards as in Europe, but a workaround was devised by establishing an agreement between them which allowed US companies to transfer and process European data if they could show they comply with the EU's stricter standards. The agreement was called Safe Harbour.

SAFE HARBOUR: A SPECIAL DEAL

4,410 US-based companies had until the end of 2015 a Safe Harbour certification. Safe Harbour was a special deal for American businesses which transfer European citizens' data to servers located in the United States. The European data protection law was not enforced directly; these companies simply had to certify they had the proper data protection standards in place. The list of US companies under the agreement included Microsoft, Apple, Google, Facebook, Twitter, Yahoo and other household names like Adobe, Amazon, eBay, HP, IBM, Intel and Oracle. In 2015 this agreement was declared invalid by the European Court of Justice through a case brought by Austrian law student Max Schrems. The decision was based mainly on Edward Snowden's revelations concerning US intelligence surveillance of European citizens whose data was processed by American companies. (See also Chap. 10)

110. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In 2016, a new Safer Harbour 2.0 agreement was negotiated under the name Privacy Shield.[111] According to the EU Commission, the new agreement puts more pressure on US companies to secure Europeans' personal data, and to create an ombudsman agency which EU citizens can direct their complaints to. But it's facing criticism for continuing to allow US companies to self-certify[112] and is expected to be rejected once again by the European Court of Justice.[113]

EU GENERAL DATA PROTECTION REGULATION 2016

As is often the case, technological developments happened quicker and with a much more transformative effect than expected. Cloud computing, social networking, location-based services, web 2.0. and, not least of all, big data and the data-driven business model quickly became an integral part of digital business. Only 17 years after the first data protection directive was adopted, European policy makers realised that reality had far surpassed the challenges they had tried to anticipate and get ahead of in 1995. In 2012, EU Member States began to negotiate a new common European data protection regulation, which resulted in 2016's comprehensive reform of the original directive.

Today's European General Data Protection Reform (GDPR)[114] has a number of new requirements for companies which process European residents' personal data. Some of the most important are:

111. European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows, European Commission Press Release, 2016.

112. Privacy Shield Adopted, But Uncertainty Remains, Proskauer, Privacy Law Blog, 2016.

113. EU-US Privacy Shield now officially adopted but criticisms linger, Tech Crunch, 2016.

114. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

FINES

Fines potentially issued to any company in violation of personal data protection laws can reach up to 20 million euros and up to 4% of a company's annual turnover. Fines are one of the most effective tools leveraged by authorities and are similar to those used in the US. The authors of the book *Privacy on the Ground*[115] have interviewed CEOs from large companies in a number of countries. They suggest that the high fine the UK data protection agency (the Information Commissioner's Office, the ICO) issued to Sony in 2013 and the transparency in terms of the size of the fine and scope of its reasoning was a great deterrent to others. Sony's data leak concerned millions of names, addresses, emails, birthdates and passwords for PlayStation owners.

ACCOUNTABILITY

The regulation also emphasises accountability. This means that the data controller must have a privacy policy, and that there is a requirement to document data processing procedures and to establish the responsibilities of employees with data processing functions.

DATA PROTECTION OFFICER (DPO)

Public institutions, companies and organisations with core operations involving data processing and systematic monitoring are obliged to appoint a Data Protection Officer (DPO): a staff member with expertise in data protection legislation that ensures compliance with the EU regulation. This person has a particularly important role in a given organisation. The DPO performs his or her tasks independently and cannot, for example, be instructed on how to carry out his or her duties or be laid off in connection with the performance of them. The

115. Privacy on the Ground in the United States and Europe, Deirdre K. Mulligan and Kenneth A. Bamberger, MIT Press, 2015.

DPO should also report directly to senior management. In addition to making sure that the company or organisation complies with the regulation, the DPO is now also responsible for educating employees involved in data processing.

CONDITIONS FOR PROCESSING DATA

Collecting and processing personal data may only be done with a specific legal purpose. The data collected needs to be relevant, minimal and absolutely necessary for this purpose. It can only be kept for the period required according to the original purpose and must be deleted afterwards. Data cannot be reused unless strictly related to the original purpose it was collected and processed for. The data controller is ultimately responsible for keeping the data secure.

CONSENT

A company or organisation must obtain the consent of the people whose data it processes. This consent must be informed in clear and simple language and it must be given freely. It's the company's responsibility to prove that an individual has actively given consent (meaning the user must take an action for it to be valid, as opposed to passive approval), and that consent must be clearly defined in relation to the data's specific use. This means that it isn't good enough to just get a user's 'OK' once and then apply it to all purposes. In addition, individuals must be able to easily withdraw their consent.

DATA PORTABILITY

With the new regulation, individuals will be able to bring the data they've provided to a company with them when they change to another service. This is called data portability, which means, as a consequence, that data must be made available in a form that can be transferred to other systems.

PROFILING

Individuals have a right to object to the profiling of their data, and companies that use profiling mechanisms on their customers' data (e.g. to target marketing and personalise services) have to make it clear that they do so. When an individual objects to such data profiling, the company is required to stop.

AGE LIMIT

Children and teens below 16 years old (unless the individual member state has lowered the age limit to 13 years) cannot give consent to the processing of their data. Thirteen is the age limit used in the US for quite some time under the COPPA regulation. Consent must be obtained from their parents, and the company should try to verify that it is actually the parent who has given the OK.

INTERNAL CONTROL OF DATA PROCESSING

A data controller must form policies and implement technical and organisational measures in a transparent way in order to demonstrate that data is being treated in accordance with the regulation.

THE RIGHT TO ERASURE (OR THE RIGHT TO BE FORGOTTEN)

People have the right to have their personal data erased (often called the right to be forgotten) and to further restrict the sharing of their information, including the right to have links and copies of data held by third parties be taken down. This can happen under certain conditions (e.g. if consent is withdrawn, or if the data is outdated or no longer needed for the original purpose).

PRIVACY BY DESIGN

Data protection by design and default is mentioned in the regulation as a precondition for the new requirements. Privacy by Design (PbD) is when data protection is built into a service or product from the beginning and not as an afterthought. PbD is described in the new regulation measures as design which, among other things, minimises the processing of personal data, creates pseudonyms for such data as soon as possible, and creates transparency in relation to its handling.

THE RIGHT TO KNOW ABOUT DATA SECURITY BREACHES

Previously, there was no requirement for private companies to let customers know about data security breaches. But there is now. Companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible, within 72 hours at the latest.

PRIVACY IMPACT ASSESSMENT (PIA)

Data controllers are required to prepare a report which evaluates the impact that data processing can have on an individuals' rights and freedoms. They must identify, understand and resolve any problems that may arise in connection with the development of products and services which involve processing personal data. A Privacy Impact Assessment must include, among other things, a thorough dataflow analysis.

DATA EXCHANGES WITH COUNTRIES OUTSIDE THE EU

The regulation does not allow the transfer of data outside Europe unless the destination country has the same data protection standards in place.

BEYOND COMPLIANCE

The International Organisation of Privacy Professionals (such as data protection officers, DPOs) was established in 2000. By 2013 it included 10,000 members and in the following two years that number jumped to 25,000 - almost all based in developed countries, where the field is clearly seeing its strongest growth. These DPOs are not just lawyers. Just 40% the International Association of Privacy Professionals' (IAPP) members are lawyers that work in organisational law departments. The rest are people who work in strategy, risk management, human resources, marketing, finance and all other posts within a business which touch data.

Robin Wilton[116], Technical Outreach Director at the Internet Society:

> **"The only next step for businesses is to move from a liability and compliance mentality to a more ethical approach, where people are doing things because it's in accordance with their values: 'Im not doing this to tick a box; I'm doing this because I think it's right.'"**

Wilton has followed the development of the data-driven business model over 28 years, 12 of them working for IBM. He believes that some fundamental socio-ethical issues are starting to gain traction and put pressure on businesses: "What does society want to achieve? What type of society does it want to be for people to live in? These are classic ethical questions that are all affected intimately now by the way in which we interact with online systems and the way that data is collected about us, processed, exploited, monetised, and so on…"

Laws are framed to include interpretations and exceptions that permit data collection beyond the norm, including for purposes such as

116. Robin Wilton, February, 2016, personal interview.

law enforcement, public safety and security. According to Wilton, "A major challenge is to ensure that such carve-outs remain consistent with what is just and fair, particularly since data use practices tend to evolve much faster than the related laws and regulatory measures."

HUMAN RIGHTS

Since the middle of the 20th century, the right to privacy has been an established universal human right in international conventions and declarations, including the UN Human Rights Declaration. In particular, since the 1950s until today, society has undergone a rapid technological evolution. The Internet has challenged and continues to challenge human rights in new ways, both negatively and positively. We have new opportunities to express ourselves and to form political communities, but also new means to surveil, monitor and censor citizens. This has meant that politicians and intergovernmental organisations repeatedly have had to revise the way we interpret expectations we have to the bodies that influence and enforce human rights, including private companies.

In her book *Framing the Net* (2013), the Danish Institute for Human Rights' Rikke Frank Jørgensen described how the political debate on the web's implications for human rights has accumulated over the years, with a momentum that has now reached its peak. For instance, we've seen this in the UN which in the 2010s adopted several resolutions reaffirming that "the same rights that people have offline must also be protected online"[117] and expressing concern over the negative impact that surveillance and interception of communications can have on human rights.[118]

---

117. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, adopted by UN Human Rights Council 27 June 2016.
118. The Right to Privacy in the Digital Age, adopted by the UN General Assembly on 18 December 2013.

The decision to establish a United Nations special rapporteur on the right to privacy, was a move which happened quickly and with much greater public fanfare than previously seen for other UN rapporteur appointments. Organisations and institutions around the globe had been asking for the UN to renew its emphasis on the right to privacy after the mass surveillance revelations in 2013, and in June 2015 Professor Joe A. Cannataci[119] was appointed the UN's first special rapporteur on privacy. Although one would assume state surveillance to be the main concern of the new privacy rapporteur, Cannataci has said he's identified several other additional issues regarding digital-age privacy implications which he will also address during his term in office[120]. At least one of these concerns relates to data held in the private sector as distinct from personal data collected and stored primarily by the public sector.

While states have gained unprecedented access to information on citizens through new, automated data storage and processing, the same can be said about businesses. Cannataci thinks that the increasing control companies gain once they possess too much knowledge about their users can be likened to that of the power balance between nations and their citizens:

"But with businesses it's a different kind of control. It is not necessarily linked to the distribution of power, but to the distribution of wealth and the exploitation of economic means, and that is where I fear the control of information from businesses."

However, Cannataci has no intention of declaring war on companies. He wishes to work with them in order to gradually push the Privacy by

119. Professor Joe A. Cannataci, November, 2015, personal interview.

120. Some of these are listed in his first report to the UN's Human Rights Council of 9th March 2016.

Design approach as a pervasive model. He sees this process as an incremental transition where all aspects connected to intrusive actions (including elements of business models) must be examined.

He also believes that most companies will be open to change some of their practices as they are starting to realise that public backlash is a real risk: "What we have witnessed over the past years is that these companies growingly gather personal data, making a lot of money, but they did not sit down and consult their clients. They could do it, they did it and they got away with it, but now we are at a stage where society is slowly waking up and saying 'is this right? Should we intervene?' Now all of the sudden the companies are being put under the spotlight and a number of them have reacted by significantly increasing privacy safeguards and especially user settings and encryption."

He noted that some of the larger companies in particular have worked hard to shed their image of surreptitious data collectors, making privacy one of their selling points: "This attempt to make privacy part of the competitive edge of a product or a service and integrate that into part of the brand's image is a significant step in the right direction."

Cannataci is looking forward to the day when more companies realise that privacy is one of the things that customers use to differentiate their product offering and therefore design them to be privacy-friendly from the start.

GLOBAL GUIDELINES FOR BUSINESSES

In 2011, the UN Human Rights Council adopted a set of guidelines for companies concerning human rights (UN Guiding Principles on Business and Human Rights). It is the global standard you would expect for corporate behaviour in this area and it specifically defines what a business (and government) should do to handle their influence on human rights. The guidelines are now part of many companies' CSR strategy*:* "Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others

and should address adverse human rights impacts with which they are involved." [121]

UN guidelines and resolutions are not laws in the sense that a company can be directly penalised for violating them, but they do hold symbolic value. They provide a general expectation as to how businesses behave, including the expectation that they respect the privacy of citizens offline as well as online.

THE DATA INDUSTRY LOBBY

The first European Data Protection Directive of 1995 was developed by a small group of experts in cooperation with national data protection authorities and received little attention from the public. In 2012, when the data protection reform was initiated, there was a whole range of interests at stake - a new, Internet-based economy, society and culture – and the existing tension all revolved around data. It was, essentially, the new economy's gold.

The EU data protection reform became a battleground for different interests. Even before the EU Commission published its first update proposal, it was subject to massive lobbying. Viviane Reding, one of the key figures behind the proposal and EU Justice Commissioner at the time, later said that she had never experienced such heavy lobbying before.[122] Several MEPs have said the same about the subsequent process.

Numerous critical arguments against the reform were about its impact on innovation. Lobbyists were arguing that the increased requirements would limit businesses' ability to innovate using data. Pressure came mainly from across the Atlantic, as American tech giants and the US government's Chamber of Commerce got involved in the reform's drafting via direct phone calls, campaigns and industry coalitions. In 2013, some even went as far as saying that the reform

121. Foundational principle 11, UN Guiding Principles on Business and Human Rights.

122. EU Privacy Regulation subjected to Unprecedented Lobbying, The Telegraph, 2012.

could potentially lead to a 'Trade War' between the US and Europe.[123]

The final version of the regulation is the result of a series of discussions and lobbying activities which included European as well as American companies, governments and organisations. A concrete example of the way the war over data resulted in an actual reform decision was the discussion surrounding the introduction of a 16-year age limit (see above). At first, the provision was that companies cannot collect and process data on children and adolescents under 16 years old without parental consent. However, the final version of the regulation establishes that each Member State may choose to lower the age limit to 13 years, which many will most likely do. On this topic, the American social media giants, among others, got involved both on stage and behind the scenes. As a British child protection expert once described it, "I was told by some of the individuals bombarding me that Google, Facebook and the US companies are 'furious'".[124] These are companies which have built their social media monopolies on European children and adolescents (and adults), and therefore have quite a lot to lose if they are restricted in this market.

In most European countries, Facebook has become a prerequisite for young people's social life. A fixed minimum age would mean that teenagers under 16 who wanted to use social networks like Facebook, Instagram, YouTube and Twitter, could only do so with parental consent. So far, American social media companies operating in Europe have followed the US COPPA law, where the age limit for the collection and processing of data on children is 13 years of age. They've done this by simply letting users specify their own age. With the GDPR age limit, however, social media services would either have to formally prohibit a large part of young people (those between 13 and 16) from accessing their services, or implement costly technologies and

123. Proposed EU data protection reform could start a "trade war," US official says, Ars-Technica, 2013.

124. We need the conversation to begin soon, Desiderata, 2016.

policies that would ensure parental consent and responsible treatment of the data.

A more general example of industry lobbying in the political data field, is the way in which Google allegedly has ties reaching far into the heart of the political processes which affect its business either by 'cosy' relationships with policymakers, funding of activities, or frequent interchange of staff between the policy sphere and the company. Sam Biddle of Intercept for example looked at a privacy conference held by the US Federal Trade Commission in 2016 to inform policymaking with research and found that 13 out of 19 papers and 23 out of 41 speakers had financial ties to Google, but only two papers included a disclosure of ongoing or past financial connections to the company.[125]

125. Tech Money Lurks Behind Government Conference, The Intercept, 2016.

Companies all over the world face new global opportunities without shared global rules on data protection and competition.

CHAPTER 10

DATA MONOPOLIES AND VALUE CLASHES

Several significant lawsuits prompting large-scale media debate and political discourse have focused on American tech giants' treatment of European law and European legislators' enforcement of it (or lack thereof). Key questions have been raised as to the legal jurisdiction of these tech companies' practices. Which rules and laws should they follow, particularly in relation to the collection and processing of data, and their practices relating to tax matters or competition challenges? Business cultures and cultural approaches have been clashing also.

Data has become a many-faceted legal issue and a cultural and intergovernmental matter. These tensions are symptomatic of the type of processes that emerge from global conditions, which in turn create conflict between local systems, laws and cultures. But new global standards and agreements are emerging. Global standards are being negotiated and roles, rights and responsibilities being distributed. The new European Data Protection Regulation will most likely be approached as a paradigm and, as such, it's already being looked to accordingly by governments, businesses and organisations around the world. In addition, the way in which data and the commercial concentration of it is viewed in the context of EU competition law (together with American anti-trust laws, the worlds' most influential competi-

tion regulation system) will establish a precedence for the way competition is negotiated internationally.

COMPETITION IN THE GLOBAL DATA ERA

> **Nettby.** In this millennium's first decade, a thriving social network called Nettby cropped up in Norway. It was an open place where anyone could create a page and publish images, express opinions and interests, and share other information. In your guestbook, friends and everyone else wrote messages, and you could read what others had written. There were thousands of groups discussing everything from politics to child care. Users were moderators or volunteers, while Nettby itself had nine employees. Over 800,000 people inhabited Nettby; it was a solid success. It's main shareholder, VG, exported Nettby to Sweden and laid out a plan to expand to the rest of Europe. But in 2010, Nettby closed.[126] One reason was that some municipalities in Norway blocked access to Nettby in schools in 2009 because students simply spent too much time on the social network. Everything started to go downhill and users left Nettby in favour of other social networks – particularly Facebook that the municipalities never blocked access to.

Nettby is one of several European social media companies that did not survive the web's first commercial chapter. In Holland there was Hyves, which had over 10 million users at its peak but closed in 2013 because its online community moved to Facebook and Twitter. In Denmark there was Arto, which, considering the country's size and e-readiness in 2007, had a good half a million users. Arto ended up a

126. Nettby, no.wikipedia.org, 2016.

ghost town before it finally closed in 2016.[127] In the UK there was Friends Reunited.[128] They thrived, struggled, then finally gave up.

Similar stories unfolded in other European nations. Though the Internet globalised the market, cultural values and laws remained local. Companies all over the world suddenly faced new global opportunities without the global rules to match, not to mention cultural values. And with so many different European languages they lacked a large, common, domestic market to grow in before going global. Some European companies consequently lost the international competition battle; they were fighting on uneven footing with companies moving forward under less strict data protection standards, innovation practices adapted to operate within legal grey areas, and more fiercely-competitive business cultures. One might argue that for many years, unresolved issues of jurisdiction and special deals, such as the Safe Harbour Agreement, created a free space in Europe, especially for the US-based Internet industry. This free space is becoming more and more restricted, however. Years – and a series of judgments and lawsuits – later, it's much more apparent that jurisdiction is not limited to the physical position of a company and its servers, but includes the places where users are located.

EUROPE VS FACEBOOK

As a result of the discussions and international pressure from the EU regarding new tech companies' jurisdictions and responsibilities towards European citizens, Facebook announced in 2008 that it was moving its international headquarters from Palo Alto in Silicon Valley to Ireland. From that day forth, the Irish Data Protection Commission became the main authority overseeing Facebook's handling of all data pertaining to European users. The Irish Data Protection Commission offices sit above a small, lonely grocery store in a minor Irish

127. Et af Danmarks første Sociale Medier Lukker, Finans, 2016.

128. Friends Reunited website to close down, BBC, 2016.

town. It has limited resources and is evidently not very well-equipped to enforce legislation which involves the protection of data belonging to millions of European Facebook users. Unsurprisingly, it has also been criticised for not flexing a bit more muscle when dealing with the social networking juggernaut. One of its most outspoken critics, Austrian advocate Max Schrems, filed a complaint, *Europe v Facebook*, against Facebook Ireland Ltd. with the Irish Data Protection Commissioner. The Commissioner rejected the complaint, and Schrems then filed an application for judicial review in the Irish High Court, which passed it on to the EU Court of Justice to assess a possible breach of Article 8 (the right to privacy) of the European Human Rights Charter. The main focus was the Safe Harbour agreement and, in light of the PRISM programme revelations, the court ruled this agreement invalid in 2015.

Along with 25,000 other Europeans and the support of many more, Max Schrems has also filed a class-action suit against Facebook regarding its privacy policy, its participation in the NSA PRISM program, data use via Facebook Graph, apps, and tracking via like-buttons, big data systems for monitoring users, and the failure to comply with user requests for access to their data. The case, also referred to as EU v. Facebook, was at first rejected by the court in Austria, which pointed out the case should be pursued in Ireland. However, it has now been brought to a higher court in Austria via the appeals process.

With the EU General Data Protection Regulation, the responsibilities of European Data Authorities have been reinforced. Each member state is to establish a Supervisory Authority (SA) to hear and investigate complaints and sanction offences, with each nation's SA helping the other's and the organisation of joint operations.

BELGIUM VS FACEBOOK

The Belgian data protection authority (the Privacy Commission) has also filed a suit against Facebook. It believes Facebook violates European data protection law by tracking EU residents who do not

have profiles on the social network through use of the DATR cookie. The Belgian Privacy Commission won its first case, and Facebook had stopped tracking non-users there, but the social media giant then appealed the case. In June 2016, the Belgian appeals court rejected the filing on the grounds that Ireland has jurisdiction – a major victory for Facebook.[129]

A number of other European data protection authorities, with the French first and foremost, support the Belgian Privacy Commission. In February 2016, the French data protection authority (CNIL) ordered Facebook to stop tracking people who do not have a profile on the site and to halt parts of their data transfers to the USA.

GERMANY VS FACEBOOK

The Germans have attempted to enforce their national data protection legislation in relation to Facebook also. For example, the data protection authority in Schleswig-Holstein tried to prevent Facebook from applying its real name policy to German citizens. The authority maintained that Germans have a legal right to anonymity, but Facebook won the case by claiming that the trial should be held on its home turf in Ireland. Later, the data protection authority in Hamburg made an administrative decision and declared that Germans have the right to use names other than their own on Facebook. The Director of the Hamburg authority, Johannes Caspar, eventually lost the case against Facebook in the German Court, which agreed that the matter should be settled in Ireland. The case's fate is now in the hands of the EU court reviewing the decision.

The Germans, however, are not letting go. In March 2016, the Bundeskartellamt, which has more resources than the local data authorities, initiated proceedings to investigate suspicions that Facebook, with its specific terms of service regarding user data, has abused its presumably dominant position in the social networking market.

129. Facebook wins privacy case against Belgian data protection authority, Reuters, 2016.

The German competition regulator is working closely with other European authorities and the EU Competition Commissioner, Margrethe Vestager. At a meeting in Copenhagen[130] in September 2016 she said:

"The German authority is concerned that Facebook may have forced its users to accept privacy terms that aren't in line with the data protection rules."

PRIVACY IN THE EU AND THE USA

European and American approaches to the right to privacy and data protection are fundamentally different. The US law professors Daniel J. Solove and Paul M. Schwartz have suggested that the difference lies in the underlying philosophy, which includes the very defintion of what personal data is, and thus in the way data protection and privacy are implemented: "Besides functioning differently, EU and U.S. privacy law have different underlying goals and different structures. As an initial matter, EU law views privacy as a fundamental right, while U.S. law considers it one interest that is balanced against others. It may even be secondary to other concerns, such as freedom of speech."[131]

In Europe the right to privacy is defined directly in several legal instruments – the EU Charter of Fundamental Rights and the European Convention on Human Rights. In addition, the EU Charter has a right to data protection, and the Council of Europe's Convention 108 is only about data protection. The right to privacy, however, is only indirectly mentioned in the US Constitution's 4th amendment, which describes people's right "...to be secure in their persons, houses,

130. Facebook privacy issues may not be competition matters, Reuters, September 9th 2016.

131. Reconciling Personal Information in the United States and European Union, Paul M. Schwartz and Daniel J. Solove, 102 Cal. L. Rev. 877, 2014.

papers, and effects, against unreasonable searches and seizures...", essentially a protection against governmental interference. The word privacy is not mentioned anywhere in the US constitution, while the right to freedom of expression is the constitution's 1st amendment and as such has generally been given more weight. Fundamentally in the United States, the right to privacy has first and foremost been defined as a consumer right and is more a question of risk management for most companies.

Data protection legislation in Europe is detailed (Chap. 9), applies to both public and private companies, and provides broad coverage with few exceptions. In the United States, the Federal Trade Commission (FTC) is the body charged with preventing "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[132] In matters of privacy, the FTC has to enforce privacy promises made in the marketplace.

In general, data protection in the United States consists of several laws aimed at specific industries. There is COPPA, which regulates the use of data on children, and HIPPA, which regulates the use of health data. There are special regulations regarding financial activities and credit companies, as well as those specific to individual states. There's also the Federal Trade Act (FTA) which prohibits unfair company practices throughout the country. The FTC (which enforces the FTA), has brought forth more than 100 cases related to privacy and data security and smacks offenders with heavy fines for unfair or deceptive practices.

American privacy regulation is based on corporate self-regulation. A company promises to treat, collect and protect data in an ethical way and the FTC only steps in, often with heavy fines, if it does not fulfil what it pledged to do. In the United States, regulation happens in retrospect, only after an issue has occurred (e.g. a hack, a data leak or other), while in the EU, the approach so far has been mostly preventive with detailed data protection laws with very low fines for viola-

132. U.S. Code § 45 - Unfair methods of competition unlawful; prevention by Commission.

tions. That being said, the new EU data protection regulation will surely bring about a change.

All in all, the difference between the two in terms of data legislation enforcement is as big as the ocean which separates them. But there has been some effort to reconcile their contrasting approaches. EU Commission Director of Fundamental Rights and Union Citizenship, Paul Nemitz, stated as much quite clearly at the European privacy conference CPDP 2015:

"In the best of worlds we would have shared European data protection rules with US enforcement."

PRIVACY PROFESSIONALS

In the book *Privacy on the Ground*, Kenneth A. Bamberger and Deirdre K. Mulligan explain how the basic difference in approach plays out among data protection and privacy professionals in the US and Europe. They interviewed professionals in charge of data protection at large private companies in Germany, Spain, France, the UK and the USA. While the Spanish tend to see privacy as legal text and an extra burden, the French are active in a way which is similar to the Germans: by addressing regulations and by making privacy a corporate social responsibility. The English in turn perceive privacy as the Americans do, as a competitive factor that can increase digital trust. The authors make another interesting observation: despite differences in their cultural environments and respective data protection regulations, German and US privacy professionals appeared to have the strongest privacy management practices. They describe privacy as an important strategic area that goes much deeper than just compliance with the law, becoming a social value and a core social responsibility.

THE RIGHT TO BE FORGOTTEN

The Internet and its search engines have created public, historical traces on individuals, providing facts about a person from both the present and the past. While this information is important for us to access all the relevant information about a person we may want to hire for a job, trade with or live next to, it can also violate that person's right to privacy.

In Europe, an individual's control over historical information in public archives has always been part of the way in which privacy is managed.

If someone has been convicted of a crime but later acquitted, he or she has had the ability to 'delete' that criminal past from publicly accessible archives and start fresh. In the US, there's a clear emphasis on the public's right to information and freedom of expression, which has been taken one step further with the Internet. Searchable digital archives on previously convicted felons and online portals that review teachers, boyfriends and girlfriends are not uncommon. The 'right to be forgotten' or 'the right to erasure' debate in Europe exemplifies the fundamental differences on each side of the pond in what level of control an individual has over his or her historical data in public archives.

In 2014, the EU Court of Justice ruled on this very issue with its 'Right to be Forgotten' judgement (RTBF). A man asked the newspaper *La Vanguardia* to remove a link to an old article about an auction notice on his foreclosed house, related to a debt he later paid. The Spanish Data Protection Agency refused his claim, but agreed to his complaint about Google's links to the article and asked the search engine to remove them. Google then brought the Data Protection Agency's decision to the national court which referred the case to the EU Court of Justice. There it was decided that Google and other search engines are in fact data controllers of the content they link to (as they are indexing and thereby processing it). Any failure to react to

such complaints and, in relevant cases, delete links to the information in question would be deemed a serious infringement of a citizen's right to privacy and data protection under the EU Charter of Fundamental Rights. Though the verdict does underline the importance of information of public interest, in essence it emphasises the individual's right to privacy via control of historical personal data. As a result of the judgment, hundreds of thousands of Europeans requested that Google remove links from its search results, which many perceive as the main portal for creating a digital profile of a person.

SALE TO THIRD PARTIES

One important difference between European and US privacy legislation is that American companies, in many areas, do not have to obtain consent to resell customer data to third parties. In the US, data on people is traded more freely by so-called data brokers, among others. In the EU, however, all websites with cookies have to obtain informed consent from users before collecting data – a rule with the good intention of informing users and ensuring their consent, but which unfortunately has perhaps ended up blinding Europeans to their right to consent, as many just tick the cookie consent box to access a website. In many ways, the whole idea of consent, heavily emphasised in the new EU data regulation, has been watered down. When you register for a website, for example a social media site, you allow it to use your data for wide range of purposes (which includes trading your data) without thinking twice.

THE NEW DATA MONOPOLY

In today's digital infrastructure, data has become a company asset. It has a status similar to that of oil, steel and railways during the Industrial Revolution, where competition law was practically invented. Although American authorities dropped an antitrust action against Google, the European Commission has been running a similar case

against Google Search for years, and in 2016 Android became a new focus area, as did Google Shopping. In essence, Google is accused of favouring its own services and thus hampering competition on its platforms, forming, in other words, a monopoly.

Margrethe Vestager[133], the European Commissioner for Competition, is particularly aware of data as a determining power factor in the digital economy: "We are not used to treating personal data as profit, and now suddenly it's a means of payment that we can't see the exact value of when we pay. This is one of the reasons why data and big data in particular needs to be viewed as an asset, an economic factor – just like we do with turnover. We need to ensure that the users paying with data for 'free services' have the same rights as when they pay with money".

She continued: "Privacy is a fundamental right and important for our right to self-determination. We must decide with whom we share our data and for what purposes. There is no price on privacy, and many say that they don't care. Personally I think that is crazy, and I think we need a legal framework that protects our data."

Vestager doesn't think that it is companies from the US where the data protection regulation is less strict that necessarily are the 'bad guys': "It's not important who owns a company or from which country it comes from. What matters is the company's conduct. We are not at war with anyone. We are looking at conduct to ensure that it doesn't have an effect on pricing or innovation in a way that is harmful to the consumer.[...]In the EU we have some considerations in regards to work conditions, the environment, tax payment and respect for data protection law. We have a European culture and a regulated market economy in Europe that considers these things. This is, in my opinion, crucial."

On face value she doesnt think that the competition law will fix the problems regarding the challenges to privacy, even with the new EU Data Protection regulation. But; "if a company's concentration and

133. Margrethe Vestager, December, 2015, personal interview.

use of data destroys competition, we will need to ensure a level playing field."

Within the past few years, European politicians have been increasingly looking at global companies' data practices as factors with a direct impact on competition. As data becomes more and more valuable, a heavier spotlight will be put on corporate accumulation and capitalisation of data. The data monopoly's effects on competition can be described accordingly:

- **Winner-takes-all.** Number one on the market takes it all, e.g. Google dominates 90% of the European online search market.
- **Closed platforms.** It's difficult and expensive for consumers to change service providers, e.g. to leave Apple's platform.
- **Acquisitions.** Big businesses acquire smaller competitors before they grow too big, e.g. Facebook's acquisition of Instagram or Amazon's of Zappos. Within the artificial intelligence field we are seeing five companies, Google, Amazon, Facebook, Apple and Microsoft, buying up most AI-start-ups.[134]

OUSTED BY 'FREE'

Between 2001 and 2005, the Danish web analytics firm Netminers was doing quite well. There were other players on the global market, and competition was fair. However, in 2005 Google acquired the US web analytics firm Urchin. Google Analytics, GA, was soon to follow: a web analytics tool 'freely' available for everyone, even for those who aren't Google's own customers. This changed the market for Netminers and other web analytics providers charging money for their services. Some of the providers went bankrupt; others managed to

134. Why AI consolidation will create the worst monopoly in US history, TechChrunch, 2016.

reinvent their services. Netminers decided to bet on the larger customers in the high-end market that Google had not yet conquered, but that was only a question of time. Today, Google controls 80% of the market for web analytics.

Netminers' CEO, Christian Vermehren[135], believes that these are unequal conditions for competition: "If you have a dominant position in a market and dump the prices below the production costs, we need to ask if this is legal according to anti-trust law. [...] The other thing is the personal data and cookie regulations. If you have Google Analytics on your site, then you can't say anything about what the purpose of your data collection is, although it's a requirement, because you have no idea about how Google uses this data. These sites should actually have a data processing agreement with Google, but Google does not offer this."

Netminers. The Danish company Netminers sells web analytics tools and offers businesses personalised dashboards with segmentation tools to optimise their websites. Although in direct competition with Google Analytics, Netminers is slightly different because customers have control over the data collected and they get a data processing agreement – required by law – with the company. After years of fierce competition with 'free' Google Analytics, Netminers are experiencing a growing interest in its services, precisely because of the need for businesses to control their data. Several Danish public institutions have chosen Netminers' product over GA.

BALKANISATION AND PROTECTIONISM

In a completely different ballpark, there's China. In July 2015, the Chinese government imposed a series of laws that encourage companies to develop products for the national market, using local suppliers.

135. Christian Vermehren, March, 2016, personal interview.

All new digital services and components which arrive from the international market are copied, developed and replaced by a local Chinese version – with Chinese governmental support. The Chinese already have their own Amazon, Facebook and Google. They have Alibaba, WeChat, Weibo and Huawei. The fact that China operates in a protectionist manner is perhaps not surprising. For years, Europe has embraced the global tech industry's local investments and even the transfer of companies from the Continent to California. But we see emerging protest. More and more Europeans are asking for equal enforcement of stricter data protection legislation. Germany and France have built their own national networks; Schlandnet and Sovereign Cloud. France also invests millions of euros in start-ups to develop the national digital infrastructure. Australia, China, India and Russia have adopted legislation barring their citizens' personal data from being moved out of the country, causing cloud companies to build data centres within local boundaries. And Germany does not want its nationals' sensitive personal data placed in the cloud services of companies headquartered in the USA.

MICROSOFT VS USA

The US government has sought to gain access to American-run corporate servers located outside its borders. But in July 2016, Microsoft won in New York's 2nd Circuit Court of Appeals, in a case brought about by the US government's demand for access to emails involved in a narcotics case. With the judgment, Microsoft has been exonerated from handing over emails or other data stored on its servers outside the United States, in this case in Ireland. The verdict is of critical importance, especially for the economic potential of American companies in Europe. The four largest cloud services in the EU are from the US and they control 40% of the entire European market.[136] Despite a

136. U.S. Tech Firms Dominate Cloud Services in Western Europe, The Wall Street Journal, 2016.

balkanisation trend, their market shares are increasing; they've built new, large data centres in the EU, large enough to offer data storage which is very cheap, flexible and – after the Microsoft judgment – also safe from NSA access. If US companies were unable to protect European data on European soil, they would be quite badly off. What remains is for the US government to ask for access via the government in the country holding the data. In Microsoft's case, Ireland said that it would have been open to help the US government, but that it never was asked in the first place.[137] Microsoft has already protected against the risk that the US government could be granted access to data on European soil by partnering with T-Systems to deliver a cloud service under German jurisdiction (Chap. 4).

137. US cannot force Microsoft to hand over emails stored abroad, court rules, The Guardian, 2016.

The Internet and data exchanges are only going to become more embedded in our physical, everyday lives.

CHAPTER 11

THE FUTURE IS NOW

In 2015, Amazon introduced a small, speaker-like gizmo for your living room called Echo to American consumers. The device can be activated by voice recognition and asked to do different tasks for you, such as play your favourite music, answer questions, put together a shopping list, turn off the lights. A bit like the built-in virtual assistants Apple's Siri, Microsoft's Cortana and Google Now.

A few years ago, IBM's super computer Watson beat its human opponents on the TV program Jeopardy! by processing and analysing large amounts of data and intuitively recognising human communication. Doctors have also used Watson to help in diagnosis, and cardiac patients use the Watson-based app Cafe Well Concierge to manage their treatment after a heart attack. They can ask the app questions about their health and physical progress and receive guidance. A myriad of self-measuring apps, i.e. wearables, measure your steps, heart rate and fertility. Some day, small chips might flow along our bloodstream and send data back and forth to tell us how we're doing. A few people already have said yes to have a small chip implanted in the wrist which does just that.

In fact, the future is here and now. The progress that we, for years, have envisioned in which everything and everyone is connected via machines and networks in a constant exchange of data is happening.

The Internet is poised to become a larger and larger part of our physical lives. Several of the things we surround ourselves with are already communicating to the web and to each other. Even our bodies are becoming increasingly connected. Through the network we plug into, sometimes knowingly but most often not, we generate vast amounts of data that is analysed and combined using algorithms in what are called 'smart' technologies. Our voices, faces, likes, interests, networks, purchasing histories, political beliefs, health, sexuality, and physical movements are already part of a larger global machine centred on predicting patterns, streamlining processes, guiding us, taking over and even controlling our behaviour.

There are five main areas that are important to keep an eye on: the Internet of Things (IoT), drones, robots, artificial intelligence and wearables. They may be seen as components of each other, and together they form the technological developments which point to the future.

THE INTERNET OF THINGS

Huawei, a major Chinese producer of communication equipment, has predicted that by 2025 more than 100 billion things will be connected to cloud computing systems, including vehicles, various types of appliances, and industrial machinery.[138] McKinsey estimates that the potential economic impact of internet connected things could be up to 11.1 trillion dollars per year.[139]

The Internet of Things (IoT) is a term that describes the increasing number of devices connected to the Internet by sensors which collect and analyse data about us and our surroundings. The category includes cloud computing systems with different types of algorithms and intelligent technologies (machine learning). So far, the term has

138. Embracing the Future and Building a Better Connected World, Huawei.com, 2014.

139. The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Global Institute, 2015

been used to mean specifically dedicated devices connected to the Internet (i.e., the computer and mobile telephone), but there is virtually no limit to the things which could be connected. Light systems, refrigerators, toys, cars, glasses, clothes, watches. The IoT is a big investment for the largest enterprises. In 2015, for example, IBM created an IoT business unit that they will dedicate three billion US dollars to in the next four years.[140]

Thingful.net. The first search engine for the Internet of Things provides a geographic overview of connected items around the world, including energy, radiation, weather and air quality devices, seismographs, iBeacons, ships and aircrafts – even Internet-connected tracking devices on animals.

Amazon Echo. Echo has sensors which can hear a voice from any direction. It streams the sound to a Internet cloud where different web services recognise and respond to the query. The information you give Echo, e.g. music playlists, flight tickets and memos, are processed in Amazon's cloud to then provide an answer or solution to the user's question, exchanging information with third-party services. The device only 'wakes up' when one says the keyword 'Alexa'. Once Echo is awake, it displays a small blue light, which users have reported as intermittently being lit up without them having enabled it. In 2015, the feeling that someone was always listening led the American teenager Aanya Nigam to paranoia, prompting her to share those thoughts and ideas on Twitter, Instagram and other social media. She feared that Echo (and perhaps her mother) was listening in on her private conversations and, after a few months with Echo, she turned it off for good and hid it somewhere her mother couldn't find it.[141]

---

140. IBM's Latest Big Bet: $3 billion on the Internet of Things, Fortune, 2015.

141. Will the Internet listen to your private conversations?, Bigstory, 2015.

Samsung Smart TV. The smart TV made by South Korea's Samsung analyses and responds to user queries using cloud computing and voice recognition technology. In 2015, the Smart TV's privacy policy was severely criticised when it came out that Samsung not only collected data and transferred it to third parties, but also listened in to conversations round the clock and collected data on an unsecured server.

Hello Barbie. In 2015, Mattel launched Hello Barbie, a Wi-Fi connected Barbie doll that listens to and records its young owner's voice, sends the data back to the manufacturer via an Internet connection, analyses the data and corresponds with the child. In addition, through an email service, parents can also receive snippets of their child's conversations with the doll. Several security experts have pointed out that one can hack Hello Barbie, and the doll has been dubbed 'Surveillance Barbie'.

There's the Internet of Things, and then there's The Internet of Everything.[142] Strategies for smart cities are being developed and implemented worldwide. A smart city is optimised and streamlined by online information and communication technologies. Often, smart city initiatives are driven by the idea of creating an Internet of Everything, where humans, devices with sensors, and other services are connected in larger communication networks. Ongoing smart city initiatives couple data from institutions and individuals to find solutions to things like a lack of parking or too much traffic and garbage. Other strategies are being proposed which focus on the health sector, presenting future scenarios where senior citizens are continuously monitored, or where people don't have to go to the doctor but may be provided consultations at home on the sofa via a screen. Singapore, New York and Lon-

142. The Next Big Thing for Tech is the Internet of Everything, Time, 2014.

don are some of the some of the 'smartest' cities in the world. They are also those with the most surveillance.

The above are examples of old towns which have been transformed into smart cities, but we are also seeing the emergence of cities that are built smart from the outset.

> **Songdo.** The South Korean city of Songdo[143] was built 'smart'. Everything within it is connected to the Internet; cameras and sensors record around the clock. Apartments are equipped with screens from which people can do their shopping, call family and friends, or consult a psychologist or plastic surgeon. Garbage goes straight down through pipes to an incinerator that also heats the houses. There are wall pads from which to control the gas, water, heating, and parking in the basement. Children go to schools where they build solar panels and use three-dimensional laser printers.

The IoT is made up of so-called 'smart devices'. They collect more data than you realise, providing a richly-detailed picture of who owns the device and whatever is in its vicinity. Typically, data is stored and analysed not on the device itself, but in a proprietary cloud.

> **Wink**. The app Wink can make your home even 'smarter'. With Wink, you can link all the various Internet-connected things in your home and manage them together from an app on your mobile phone. You can remotely control lights, thermostats and door locks, all from one place. Data analyst Charles Givre has revealed what each Wink app knows about its user: Facebook and Twitter ID, precise location, all associated smart devices (the ones connected to Wink), ISP and the specific times during the day when the owner is home or away.[144]

---

143. Den Kloge By, Markus Bernsen, Weekendavisen, 2015.

144. What does Your Smart City Know About You, Charles C Givre presentation, 2015.

According to Bill Briggs, the CTO of Deloitte Consulting ″The solution lies not in the Internet of everything but rather the Internet of some things".[145] A company need not collect all data through all things, in an avalanche of useless information. It shouldn't attempt to collect every bit of data just because it can, but rather keep specific scenarios in mind and connect "with care", Briggs points out. Not all devices need to be Wi-Fi connected. If they are, there's a greater risk of security and privacy breaches and, thereby, a breach of trust with customers.

DRONES

Drones are on the minds of many. Not just the flying military machines we know from American warfare, there are also those used by journalists and researchers, those used by businesses for delivery, and even a selfie-drone, the selfie-stick's biggest competitor.

A drone is an unmanned aircraft. It flies partially autonomously through built-in computers which communicate with a remote control. All major technology companies are working with drones in some way. DHL and Amazon[146] are testing package delivery drones and IBM's IoT initiative focuses on 'precision agriculture' supported by drones that collect weather data. Aquila, Facebook's large but lightweight drone for Internet.org, will connect five billion people to the Internet – and to Facebook, of course.

The drones used by hobbyists, journalists and researchers are usually very small and may be used for various purposes. The small selfie-drone Lily is designed to follow and film, in HD quality, its owner by way of a tracking device that he or she wears on the wrist. Lily can fly a maximum of 15 meters into the air, but other drones are being brought to even greater heights to, for example, determine the num-

145. The Internet Of (Some) Things, Tech Crunch, 2015.

146. Making deliveries with the DHL Parcelcopter 3.0, DHL YouTube channel.

ber of participants in a demonstration or to look for poachers in the rain forest.

Drones can fly high and, through cameras, add a new perspective, revealing a world of details. They are unmanned and collect data that is instantly transferred via the Internet. It's far easier to imagine the challenges that a drone flying outside your window or landing on your lawn poses to your privacy than it is to understand the privacy implications of big data in general. Twice in 2015, a drone dropped down on the White House's lawn in Washington D.C. Both times it happened by accident, with two different men testing out their hobby drones. Celebrities are even pursued by paparazzi drones. In January 2015, a man in New Zealand was sitting in his living room when a drone, which turned out to be his neighbour's, snapped pictures of him through his window. The police informed him that they understood his (and others) complaints about drones' impact on privacy, but that at the moment they weren't regulated by local legislation. The man was frustrated; what could he do, what were his rights? If he were so compelled, could he shoot down the drone the next time it flew by?[147]

All over the world, drone regulations and ordinances are being developed. American authorities have repeatedly stopped Amazon from testing drones to deliver packages, and the US and Europe have both published detailed guidelines for commercial drone use. But questions about the responsibilities, roles, and implications they raise for privacy are still unclear.

MindDrone. At the Global Cyberspace Conference in the Hague in April 2015, one of the Internet's founding fathers Vinton G. Cerf managed to control a drone with his mind. He could, without having tried it before, move the MindDrone up and down from a table. The body is the very last barrier we have to protect our privacy, our innermost thoughts, needs and dreams. If a drone can be controlled with our brains, what

147. Drones Invading Privacy say Critics, Stuff, 2015.

happens when the process is reversed and our thoughts can be controlled by drones? The people behind MindDrone – the Dutch company SURFnet – believe it will be possible in the future.

ROBOTS

We are all familiar with robots from science fiction films and literature. Both evil ones and good, funny ones. There are robots like C3PO and R2D2 from Star Wars, made of metal and twinkly buttons, which speak, squeak and beep. They have personalities just like humans but look like machines. And then there are the robots which deceive us into believing they are human. It's often those we feel the most uncomfortable with. Terminators, for example, look like real men, but you soon find out that these sinister robots have cool, calculating programmed behavioural patterns without human emotion and empathy. The Swedish TV series Äkta Människor (adapted into the American television series Humans) depicts a future in which a special man-robot hybrid, the Hubot, exhibits and acts on a wide spectrum of human-like emotions. They even have an emerging 'free will' and start demanding the same rights as 'real humans'. 'Cyborg' is a term that has been used since the 1960s to describe a person (or organism), whose senses and body have been reinforced or restored using technology.

In a way we're all cyborgs, and we become increasingly so as technology becomes a greater part of our bodies and senses. Glasses amplify our sight as do contact lenses; the mobile phone in hand gives us immediate access to each other and to virtual information. The artist and cyborg activist Neil Harrison was the first man in the world to implant a Wi-Fi antenna in his skull. He was also authorised by the British authorities to have the antenna in his passport photo when he argued that it was part of him. Harrison fights for other cyborgs' rights and is also behind the Cyborg Foundation, a worldwide non-profit

organisation that enhances the body's senses through the addition of various technologies.

In science fiction, the robot is, at its core, an existential question: What makes us human? What constitutes human intelligence? The robot becomes a competitor to mankind's dominion of earth. To what extent can a machine take over human functions? Can it think and act independently, outside our control?

Yet robots are far from being just science fiction. Many kinds of robots are being developed with a wide range of functions and purposes: industrial robots, military robots, educational robots, collaborative robots, research robots, service robots and robots to talk with as an alternative to friends, family and therapists. Tiny nano robots that can destroy cancer cells are also on the way. A report from the Investment Bank of America Merrill Lynch estimates that the global market for robots and artificial intelligence will reach 152.7 billion dollars in 2020. It also predicts that robots will not only streamline a number of processes, but also they will increasingly take over jobs performed by humans today. According to the World Economic Forum, 5 million jobs will disappear because of robot technology.[148]

> **The Robotics Challenge.** The idea about the Internet was developed in the 1960s in the US military research unit DARPA. From 2012-2015, the very same unit, which developed the world's first internet, the 'Arpanet', was behind The Robotics Challenge. Grand prizes were awarded for robots which completed in a number of tasks related to disasters. Large metal robots with legs and arms, developed by 23 teams from around the world, battled to be the best car drivers, to open and go through doors, to use a tool to drill holes in a wall and walk up stairs.

The European Commission provides funding to over 100 robotic projects and estimates that the robot industry will reach between 50

148. The Future of Jobs, World Economic Forum, 2016.

and 62 billion euros in 2020. Robots have become so mainstream that there's even a social network for robots, the app-store myrobots.com, where you can connect and exchange information with other robots.

In the Western world, the focus is on machine-like robots which act as tools in our everyday lives, such as self-driving cars. In 2010, Google started testing one, the Google Car, which works by scanning its surroundings, making a 3D model and then creating routes that respect local traffic laws and detect obstacles in real time. Other manufacturers of self-driving cars have followed: Chinese Baidu, American Tesla and German Audi – not to mention American Uber.

When the idea of self-driving cars was first launched publicly, the discussion revolved around if and how robot cars could imitate human functions and judgement. There is no doubt that a computer-controlled car would be safer in many respects than a human, who is easily distracted by a stressful situation, a phone call or even tempted by alcohol. But the ethical implications are abundant. Who is faster at spotting a dangerous situation in traffic? Man or machine? Who should the self-driving car kill when it has to make a decision in a split second: the person in the car itself, the driver in the oncoming vehicle, or the child on the roadside? Who is responsible for an accident? The driver, employee, business management, the authorities?

What is the perfect algorithm for the autonomous car? Should it be designed from an individual or societal perspective? Or from a commercial one?

Certainly self-driving cars can be designed to make them independent of the Internet. But if we are to learn from them, data collection about our behaviour is important. How can this be done with fully-informed consent and in an ethical manner? As of writing, these cars are far from perfect. In 2016, the first fatal accident happened with a when a Tesla car in auto-pilot mode failed to distinguish between a white

truck and a bright sky. The brake was not applied, and the car ran into the truck.

> **Chatbots**. When Microsoft launched its English-speaking chatbot, Tay, in March 2016, the company got a proper schooling.[149] Tay was meant to engage 18-24 year olds on Twitter and become wiser and wiser in conversation with humans. But within 24 hours, Twitter users managed to corrupt Tay so that it began to pour out the most racist and inappropriate tweets possible. Microsoft shut Tay down immediately and apologised. The company had otherwise been successful with Chinese Xiaoice, which over 40 million users in China talk to about everything from light-hearted, everyday chatter to deeply troubling matters. Xiaoice is described as a 'girlfriend app'. She, like Tay, is based on machine learning technology and has a memory that allows her to remember what you previously told her and thus follow up on or tap into past conversations. Microsoft would like to develop her for commercial purposes, so she can also function as a shopping agent.

In Japan, there's a special focus on humanoid robots. Shoppers at the entrance to Tokyo's Mitsukoshi mall in April 2015 were greeted by the smiling Aiko Chihira. Chihira is a female robot developed by Toshiba. She speaks Japanese, but can also be programmed to speak other languages. And she's not the only one. Japanese robots are often crafted to understand and recognise human patterns. They're built as humanoid communication partners that analyse and understand human relations and communication. The first Japanese commander of the International Space Station had a robot companion with him called Kirobo. Kirobo can recognise voices and faces, converse, and remember things, and was built to study human and robot relations.

---

149. Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter, The Guardian, 2016.

ARTIFICIAL INTELLIGENCE

In 2011, a machine beat two people in Jeopardy!. Not just any old competitors, but Jeopardy! grandmasters. The machine wasn't present in the TV studio, where the game was recorded, because its cooling systems made too much noise. But it was there in spirit, in the form of its developers' logo, IBM, and the sound of a mechanical voice that responded to the host's answers with the correct questions. The machine is called Watson, and today represents IBM's main efforts in a field it calls cognitive computing, also known as machine learning, deep learning, intelligent technology or artificial intelligence (AI).

In 2016, Google DeepMind's AlphaGo beat the world champion in the Chinese board game Go, causing an uproar in the race between artificial and human intelligence. AlphaGo managed to find strategies different than those any human could come up with. AI machines or software are designed to mimic human intelligence. We're moving from a paradigm where a computer is something we program, to something which is capable of independendt learning. Meaning we stop telling the computer what to do, but instead give it a target, feed it with training data and then let it observe different types of events and situations to help it understand patterns and relations. Watson, like AlphaGo, is a machine which behaves intelligently by receiving information, processing it, analysing patterns and acting on them independently. In Jeopardy!, for example, Watson proved it could process and analyse complex human communication.

Watson, Google's DeepMind, Facebook's Deeptext, Microsoft's Tay and other intelligent technologies evolve, like the human brain, based on experience.

The more data the artificial intelligence machines absorb, the better they get at recognising patterns to react to.

Data flows through these machines' nervous systems – a nervous system made of programmed algorithms. They enable the machine to

coordinate actions and transmit signals to and from its various parts. Everything according to the purpose it was built for, be it to lead a passenger safely through a busy city, to inspect an area struck by an earthquake, to chat with a lonely person, or win a game.

An algorithm is, in essence, the way a computer processes data – like a knitting pattern. It's a set of pre-programmed rules; a step-by-step set of operations that the computer must perform. Algorithms can learn and evolve over time.

If data is today's gold, then the algorithms are the goldsmiths. Robots are nothing without data, but data in turn is nothing without algorithms. Thus, rather than focusing on the Big Data Economy, we need to start focusing on a new type of Algorithm Economy.[150]

Corporate proprietary algorithms embody the true value of data-driven companies. Just think of Google's search algorithms or Facebook's newsfeed algorithms. And because they are imbued with such value, these algorithms are also such companies' biggest trade secrets. Needless to say, all major tech industries are investing heavily in research and innovation in machine learning and artificial intelligence.

> **Google Brain.** Google Brain is Google's artificial intelligence research project, launched in 2011. It evolved and, in 2012, the *New York Times* reported that a cluster of 16,000 computers, created to mimic human brain activity, had trained itself to recognise a cat based on 10 million digital images taken from YouTube videos. Besides its own research and development, Google's Artificial Intelligence and Machine Learning Research department, as it's formally called, has a programme to provide support to students and universities, working with teams in Japan, China, Australia, New Zealand and India.

The largest international ICT companies are deeply aware of the algorithmic economy. They hire, on a large scale, employees in the field and all are in the process of making history in different markets.

150. Algorithm Economy, Gartner, 2016.

Google generally dedicates a large part of its budget to efforts in artificial intelligence and to the development of algorithms. The company bought the British AI start up DeepMind in 2014 for 500 million dollars. IBM plans to invest more than 1 billion dollars over the next few years and dedicate more than 2,000 employees in order to bring Watson's services to the market. So far, IBM's focus has been on the health industry, but recently its interest has begun to spread to consumer services. At the same time, one third of corporate research efforts are being put into advancing Watson.

> **OpenAI.** A group of billionaires, including Tesla's Elon Musk, PayPal's Peter Thiel and LinkedIn's Reid Hoffman, have established OpenAI. Concerned that commercial self-interests in artificial intelligence could have adverse effects if computers become more intelligent than humans, OpenAI is a non-profit research company with a mission to use AI to help humanity.

The algorithms developed in the industry and by universities can both understand and recognise spoken, written and visual communication with the help of voice and facial recognition technologies. In addition, they continue learning based on the data they're fed. A machine learning algorithm associated with the Internet could, as an example, go through the entire Internet from social media content to the news. Some can find pictures of the same person online. At some point in the near future, they'll be able to recognise someone across services and communication modes and put together an even more detailed personal profile of him or her.

There's already a start-up community developing services built on algorithms which can assemble, analyse, predict and act on data. The biggest names in AI (Amazon, IBM and Google) currently offer their learning algorithms for free to developers so they can invent new services (App developer clouds, as some of them call it). In 2015, for example, Amazon Web Services (AWS) opened a new option where, for a 12 month period, developers can freely use Amazon's algorithm

tool to analyse and predict patterns in data from various services and applications.

> **Unitesus.com**. "Custom build your perfect employee based on personality, experience, values, skills and company cultural fit". Unitesus is a Watson-based service that employers can use to find new hires. In a Reddit post[151], Unitesus CTO and co-founder Bardia Nikpourian described how instead of having to answer a personality test with 60 questions, now job candidates can simply provide social networking media content or things they wrote themselves. Watson's technology is used to analyse the provided data and create a personal profile, which is then matched to the open position and the company's profile and corporate culture.

WEARABLES

We share data about ourselves every day via Internet-connected technologies. They're all around us, but several have moved closer in on our bodies. The landline telephone was once in the living room, now the mobile phone is in your trousers' pocket. The fitness tracker touches the skin on your wrist and senses your pulse. Wearables are tech-based items which we carry close to our bodies at all times and which can help us improve or measure our physical state. As revolutionary as it may sound, it's not a new concept. Man has always tried to improve the body with the help of technology. A prosthetic leg helps the one-legged man walk, glasses help the near-sighted see. Today we have small, Internet-connected computers we can wear to monitor our health or watches and glasses that can help us identify what we see, remember it, and find digital information directly related to our view.

---

151. UnitesUs - Giving IBM Watson a Job, Finding Jobs, Reddit.com, 2015.

Fitbit is one wearable used to monitor personal health. With Fitbit you can count how many steps you've taken during the day, see how well you slept, and measure your pulse and heartbeat. But Fitbit has a bad reputation concerning its handling of sensitive personal data. For example, in 2011 a number of Fitbit customers were surprised to learn that information on their sexual activity was searchable on Google. Ductch TomTom, on the other hand, has a smartwatch with the same capabilities as Fitbit but with careful focus on privacy (see also Chap 4).

Other self-measuring apps are used by women to track fertility. The US-based Glow and Kindara programs are somewhat risky, given that fertility data – that is health data – in the United States is only regulated when squarely in the hands of insurance companies and doctors. That very same data, when used in an app, is only regulated under consumer laws with a much lower level of protection.

> **Clue.** The Berlin-based fertility tracker Clue helps women and men monitor fertility and provides new insights for reproduction and health research. Clue is aware that this is extremely sensitive data, which is why the company's privacy policy is comprehensible to the layman and not written exclusively by lawyers, for lawyers. It's possible to use the app without an account, meaning Clue has no idea who you are, where your cycle data is on your gadget, and, if you erase your data or lose your phone, your info will be deleted completely. Users can also create an account – the data from which will be anonymised for clinical and academic research – and use their data for data visualisation and creating predictions about one's cycle. The same cycle data is stored separately from personal information, which ensures an extra layer of anonymity. Lastly, but of no small importance, the company is located in Germany where the authorities have strict data legislation and also enforce it.

Many people share their data, some involuntarily and without knowing it, others more willingly. For years, American data researcher Sara

M. Watson has studied those who make up what is referred to as the Quantified Self movement, which consists of people who make great use of personal tracking technologies to monitor and improve health and physical development. It's a group of individuals which have truly gone all the way with technological developments. Sara M. Watson sees them as examples of the kind of man-technology hybrid that we're moving towards. Plus, they have insight into their data identities that many others today don't. Unlike ordinary consumers, people in the Quantified Self movement are more likely to complain that they don't have access to their data, and that data is locked within proprietary platforms and interfaces. They have also been among the first to feel the effects of very intimate details suddenly entering more public platforms. They want to exchange data, but not with everyone and via everything, preferring to remain the sole owners of such information.

SINGULARITY

In the 1990s, one of the world's great inventors and futurists, Ray Kurzweil, came up with a number of predictions about advances in future technology. Self-driving cars, glasses with internet-connected monitors and portable computers. In 2009, he estimated that 86% of them had proved to be correct. In 2015 at the annual Exponential Finance Conference in New York, he speculated that by 2030, the human brain will, by tiny DNA nanorobots, be connected to cloud technologies made of thousands of tiny computers exchanging data with each other. The technology will change our intelligence, and we will be able to do things like make a backup of our brain: "Our thinking then will be a hybrid of biological and non-biological thinking", he said. The larger and more complex such cloud technologies become, the more advanced our brains will be.[152]

In a number of books, Kurzweil has described the philosophy behind the Singularity movement. Singularity is the belief that techno-

152. Ray Kurzweil: Humans will be hybrids by 2030, CNN Money, 2015.

logical development is moving towards a non-biological, advanced, potent super intelligence, which will also enable us to transcend our biological limitations and create a new type of civilisation.

The development is, according to the Singularity movement, inevitable and we should therefore meet it with open eyes and arms. Kurzweil predicts that Singularity's idea of super intelligence will become a reality by 2045 and he thinks that we may as well manage this development. Kurzweil is also Director of Engineering at Google, heading a team developing machine intelligence. The company itself is one of the world's largest-data driven organisations, close to being a global super intelligence. The question remains, however, what the status of the individual will be in new, global, super-intelligent systems, and who or what ultimately will be managing their development and have ultimate control?

WHERE DID THE HUMANS GO?

There are many ways to describe data in business. There's big data, small data, long data, predictable data and targeted data. There's sensitive, private data, that is, personally identifiable data. Data, at its core, is also human beings. In 1964 professor Marshall McLuhan, wrote that media are extensions of ourselves. All new technologies are designed to enhance humans' physical, social, psychological and intellectual functions, and therefore they also shape our world in new ways.

Borders between the physical and digital are gradually disintegrating and there's a battle going on between big tech powerhouses for domination of the systems through which we connect to each other and to our various technologies.

From a business perspective, there are endless potential systems that effectively connect customers, companies, technologies and data with each other. From an individual's perspective, it's less straightforward.

First of all, there are a number of security risks associated with increased data collection: the next generation of hacks in the health

sector, hacks to public and private databases, hacking of drones and robots. It's an area which is becoming more and more interesting for criminals who see great financial potential in data's black market. Built-in sensors, microphones and cameras also pose new opportunities for surveillance and spying within a given industry and between countries.

But the biggest risk lies in the unequal balance of power that the opaque data market creates between individuals and corporations.

While the individuals are becoming increasingly transparent in these new digital super structures, the powerful are becoming more and more closed off.

Professor Frank Pasquale describes a society governed and controlled by secret, invisible algorithms. They permeate the entire society and are progressively essential to everything from financial markets to an individual's life. Algorithms process our digital data and can create (or destroy) our reputation or determine our fate, explains Pasquale. And this happens invisibly without people having any insight into the interests and intentions that lie behind them, without any knowledge of how such data is used, for what purpose and with what consequences it has for them as individuals.

Julia Powles, from the University of Cambridge, is particularly known for her critical articles in the *Guardian*. She looks to technological developments with concern, pointing out that innovation in IoT and big data is being driven towards centralisation, domination and control. This control is not in the individual's hands, but rather in those of the industry and the company providing the service.

HUMAN EMPOWERING SYSTEMS

Data expert Sara M. Watson questions whether technology supports the powerful data industries or the individual human. Data is not gold, capital or profit, she says. Data is blood, an individual's virtual DNA, body and fingerprints. Data is humans. If we understand data as something that points back to the individual, we can also change the way we design systems and administer the rules that protect us. If we begin to understand our data as our own and not as pieces in a grander industrial and technological machine, we can create systems which are transparent and which grant control to the individual.[153]

Technologist and cultural critic Cory Doctorow said roughly the same thing when he dreamt of an Internet of Things where people are the 'sensors' and not just data to be 'sensed'. The problem with the Internet of Things as it stands now, he posits, is that people are simply percieved as another 'thing' in a network of things that can provide data to be collected, analysed and used to create a 'magical' world around us.[154]

Critics are also concerned about a technological and industrial progress' meta-narrative. Where is such development going? In a more human direction or that of powerful industries, states, and even intelligent machines? How will private, personal lives survive in tomorrow's Internet-connected world? How do we ensure a democratic balance of power where individuals have control over their online data and insight into the processes behind its collection? One answer is to create a new infrastructure that fundamentally respects privacy and individual choice and control, which can only be accomplished through technical, legal, cultural and organisational initiatives.

153. Data is the new "....", DizMagazine, 2015.

154. Cory Doctorow: What if People Were Sensors. Not Things to be Sensed?, Locus Online, 2015.

The Council of Europe Recommendation on an Internet of Citizens. In 2016, the Council of Europe, which administers the European Convention of Human Rights, published a recommendation to all Member States concerning the Internet of Things. Interestingly, the Council chose to call it a recommendation for an 'Internet of citizens' emphasising that technological advances where things and people are increasingly connected via the Internet will simultaneously require a focus on human rights, "believing that this significant development should be complemented by an 'Internet of citizens' who are aware of their rights and responsibilities". The Council of Europe highlights the right to Freedom of Expression, privacy and data protection as particularly important focus points in such developments.[155]

Bitcoin is a type of virtual 'currency'. The digital payment system was launched in 2009 by the then-anonymous Satoshi Nakamoto. Bitcoins can be used, like normal currency, to pay for products and services online. The difference is that bitcoins are not administered centrally by a bank or government, because the blockchain system, containing an overview of distributed bitcoins, is decentralised. All bitcoin owners have a copy of the system, and each bitcoin owner has his or her own bitcoins in a digital 'pocketbook', which is not linked to their address, name or other personal information.

Blockchain. According to the proponents of the blockchain technology, it can create the trust that, in the existing online infrastructure, is missing between two parties who do not know each other. It does so in a direct, secure transfer between two parties (without the need for third-party verification) through an

155. Recommendation CM/Rec(2016)2 of the Committee of Ministers to member States on the Internet of citizens.

encryption solution that ensures each transaction is unique and non-manipulatable. The technology is open-source and can be described as a network that's spread out on all users' computers without anyone having the ability to delete or change it – a bit like a global spreadsheet. Each transaction creates a new line with a unique ID in the open, un-editable spreadsheet. Blockchain technology is expected to revolutionise the central bank systems in the same way email made post office monopolies a thing of the past.

Ethereum sees more general potential in blockchain technology.[156] The company's goal is to develop technically decentralised infrastructure, which by default and in its design is controlled by the users themselves and not by states or companies. ETHERUM, financed through a bitcoin crowdfunding campaign where it received 30,000 bitcoins (about 12 million dollars), launched in 2015. It's working on bitcoin-based platforms that will replace the World Wide Web.

Within the last few years, we have seen a number of initiatives that are, as a whole, a step towards a new, decentralised and transparent digital infrastructure which gives individuals control over their own data. This movement can be described as one which focuses on 'human empoverment'.

156. Ethereum.org, 2016.

New types of infrastructure with Personal Data Stores aim to provide individuals with control over their data.

CHAPTER 12

PERSONAL DATA STORES

Imagine you get a reminder on your smartphone whenever it's time to take your medicine. Imagine you can optimise your personal finances by linking your credit card information with electricity and water bills, rent, bank accounts and your calendar. Imagine you can fight jet lag by matching your sleep patterns and health to your travel plans. Or that you can connect thermostats in your home to your calendar, location data and weather data, ensuring your house is heated and ventilated in accordance with local weather conditions Or that you can sync shopping lists and location data to get an alert when you pass a store that has just what you need.

There are many ways we could harness our data in our favour, as individuals. But in today's digital infrastructure, commercial companies and states control this information and decide, on our behalf, what's relevant to us. In short, personal data is primarily for the benefit of industry or the state, rather than of the individual.

A movement to change the system in which people are transparent and have little control over their own data is gaining momentum, aiming to wrest control from large corporations and give it back to the individual. However, it's so new and varied that there's no agreed-upon term for it yet; it's been called everything from Personal Data Stores (PDSs), the My Data Movement, The Internet of Me, SelfData, Personal Information Management Services (PIMs) or Vendor Rela-

tionship Management (VRM, the opposite of Customer Relationship Management, CRM). Besides being an emerging market at times driven by clear commercial interests, it's objective is to provide individuals with control over their data, be it related to health, finances, travel, housing, or shopping.

In this new infrastructure, international corporations, smaller companies and the public sector will remain major players, while a framework is created in which a different kind of middleman stands between them and individuals, as stated in *Personal Data Stores* (PDS), a report published for the European Commission by the University of Cambridge.[157]

A Personal Data Store is as technology which enables an individual to gather, store, update, correct, analyse and share his/her personal data.

Of particular importance, according to the paper, is the individual's ability to give or withdraw consent to third parties' access to data. You essentially 'set' your own default privacy settings.

> **MIDATA.coop** aims to enable individuals to securely store, manage and control access to their personal data. Users will be able to give personal data to companies, scientists or a babysitter, but will be the only ones with a key to that data. MIDATA is part of the digital cooperative movement and is based in Switzerland. Its shareholders decide what charity the co-op's profits should go to. Though not yet launched, MIDATA.coop is engaged in a number of pilot projects.

157. Personal Data Stores, Guillaume Brochot, Juliana Brunini, Franco Eisma, Rebekah Larsen, Daniel J. Lewis (students), Jin Zhang (Academic supervisor), University of Cambridge for the European Commission, 2015.

Zurich-based professor and geneticist Ernst Hafen[158] is the director of MIDATA.coop. He was motivated to create the project in 2008, when he shipped his saliva to 23andMe, one of the world's large private companies collecting DNA from individuals, which is also partially funded by Google. He wanted to make use of the DNA service, but he disliked the model in which we give away our data to large corporations without retaining rights, without transparency, insight or even profit. It's not a sustainable economic model, but MIDATA.coop could be, according to Hafen, who belives that personal data cooperatives will democratise the data economy.

University of Cambridge researchers also have great faith in a PDS industry. If it suceeds, it will restore the balance of power between companies and individuals, boost consumer confidence, create new big data research opportunities and facilitate savings in the public sector, they say.

The author of *The Cluetrain Manifesto*, Doc Searls, boosted the movement with his 2012 book *The Intention Economy.* He also leads a project at the Berkmann Centre at Harvard, ProjectVRM, which was started to provide consumers with control over their data in vendor-customer relationships. Searls sees an end to Internet marketing as we know it because people are getting fed up with faulty personalised adverts based on data monitoring. They're starting to demand control and act accordingly through ad blockers – and the market is following suit. Customers have thus gained what he refers to as "bargaining power with advertisers and publishers."[159] Through ProjectVRM, he hopes to improve markets by equipping customers with the tools to help them not only be untied from vendors, but also to better engage with them.

158. Ernst Hafen, September, 2015, personal interview.

159. The End of Internet Advertising as We've Known It, MIT Technology Review, 2015.

HEALTH DATA

The health sector in particular is one area where we see the advent of PDS systems. Health data is sensitive data, and strict protection and consent requirements are in place. At the same time, it's often information individuals are extra reluctant to share. This type of data is stored in various public systems that don't 'talk', and correlating it is quite a challenge. With sensitive data, there are obviously large privacy risks. But the use of health data also shows great potential for the future, including personalised cures and research in medicine and diseases.

Healthbank.coop. "We empower people across the globe to exchange their health data on our uniquely neutral and independent platform. Healthbank drives innovation in health sciences, from prevention to cure, at a better price with better quality for the benefit of both the individual and society." These are the words from the citizen-owned health data exchange platform, Healthbank.coop. Data is secured following Swiss regulations and located in Switzerland. It went live August 2016 for a selected group of people in the initial phase.

Data for Good Foundation. The non-profit Data for Good Foundation seeks to provide a platform to gather people's health, injury and relevant behavioural information and pair it with social data such as education, employment, weight, age, residence, hobbies and applicable self-measuring data such as blood pressure, sleep and steps per day. All this data will be accessible and controllable by the individual to improve his/her lifestyle. Insurance and pension funds, municipalities, researchers and other third parties only get access to the data in an anonymous form. In this way, they don't get identifiable information, only insight into patterns. The Data for Good Foundation thus hopes to ensure that micro-tariffing, i.e. the

calculation of premiums for individuals, is done ethically and that the principles of solidarity among insurance and pension funds are not lost.[160]

Health isn't the only industry experimenting with the My Data/PDS ideas. The energy consumption sector is working with them as well.

SaveaWatt. New Zealand-based SaveaWatt has developed an intelligent digital servant named Frank which learns about consumers' energy consumption and location and matches it with a provider, who then finds the best offer for the lowest price.[161] The PDS – ensuring that individuals own their own data – also helps users change providers, if necessary. It's easy, they say, because Frank enables uniform technological standards. SaveaWatt started with power companies, but plans to expand to other areas – especially those poised to be privatised.

UNDERSTANDING THE DATA ECONOMY

Different PDS services highlight the various advantages of a new structure designed to directly benefit individuals. They all underline 'individual empowerment' as a benchmark for the development of their services and products, such as the ability to determine a personal privacy level. Individuals should be able to control what they want to share and what they don't.

PDSs are also about providing consumers with the tools necessary to switch between different providers. Some PDS services emphasise the data economy aspects ('data is capital') and offer consumers the opportunity to earn a profit on their data. They want to give individu-

160. Co-founder Annemette Broch, August 2016, personal interview.

161. Time to get FRANK on energy prices?, Ctrl Shift, 2015.

als the chance to decide when and what kind of data is used to pay for benefits and services.

Businesses developing My Data/PDSs want to provide users with a clearer understanding of the data economy and the value of their data, which currently is a grey area to the individual but obvious to the data industry.

Many are pointing out that better-personalised services will come out of the advancement of PDS since empowered users can ensure their data is accurate and up-to-date and influence how services and features are prioritised instead of passively viewing the opaque and incomprehensible personalisation algorithms of Google's search engine and Facebook's newsfeed.

The discussion around the PDS movement also highlights a number of benefits for providers and society as a whole. A new infrastructure which is more transparent and where users feel in control of their data can enhance digital trust and growth. It can provide scientists with better data, as information controlled by individuals tends to be more correct. All in all, there will be more data, deeper data, and, last but not least, true data, as opposed to that harvested online or through social media platforms like Facebook and Twitter, where the number of users who fake their data is on the rise.

In addition, small and medium enterprises can get data analyses delivered to them for less than if they had to obtain it themselves. The question remains, however, if these benefits can be brought about smoothly. PDSs demand a lot from individuals who have to familiarise themselves with their own data – not least fully grasp the value of it. At the same time, it also requires them to understand the implications of sharing their data. It may work for well-educated individuals, but there is also the possibility that in the new infrastructure, new digital divides will form between those who understand and can use their data for their personal benefit and those who cannot. According to the authors of the Personal Data Stores report published for Cambridge University, there are two possible scenarios: either PDSs will increase trust and thus people's desire to share data, which will in turn benefit

growth, or they'll be used to lock in personal data completely. What happens next also depends on consumers' willingness to prioritise privacy and personal control over convenient, inexpensive services.

COMMERCIAL PERSONAL DATA STORES

According to British consulting firm, CtrlShift, which specialises in Personal Information Management Services (PIMS), the new industry is growing rapidly. We're hurriedly moving away from the traditional B2C business model to a new Me2B concept[162] where information no longer comes from above, but from below, or even peer-to-peer. If the Me2B market takes hold, the large, traditional B2C platforms like Google, Facebook, Twitter and LinkedIn (which run on voluntary data submission from individuals) will come up against quite a challenge. At the same time, the cost of collecting, storing and sharing information has become so low that individuals are now able to do what big companies once built their growth upon.

Akin to the emergence of non-commercial PDSs like MIDATA.coop, we are seeing a resurgence of commercial PDS services. They too aim to provide individuals with control over their data, but have added the opportunity for people to make money on it. A thriving start-up community to give individuals tools to commercialise their own data seems to be cropping up in the UK in particular.

> **Citizenme.** This British PDS offers insight into your financial situation to share your info with companies that want to know more. Everything from your Facebook likes to your zip code is merged in Citizenme, and only you have access to your data. Citizenme does not store data nor can the company see your info unless you allow it to, based on the principle that you want to be paid for companies gaining insight into such personal statistics. In other words, you are essentially paid to take part in

162. The Me2B opportunity, Ctrl Shift, 2015.

user and opinion polls. The PDS is European and thus subject to EU data protection legislation. According CEO and founder StJohn Deakins[163], Citizenme is making an extra effort to convey its privacy policy in a way that's understandable for those of us who aren't lawyers.

Mydex. This British platform promises it will remain independent, never be sold to a state or a multinational company, and that 65% of its earnings will be invested in social purposes. Mydex is more than just a PDS where individuals can collect all their information in one secure location, such as passwords, emails, addresses, social media logins and credit cards. It's also working with the UK Data Protection Authority, ICO, and gathers personal data from municipalities, energy companies and hospitals in an effort to create a secure personal data exchange, rather than being done by just one public institution. The platform is ISO 27001 certified and operates with Privacy by Design principles.

Synergetics. "So far, organisations have been taking personal data unchecked. Without your consent," says the Director of Synergetics, Luk Vervenne, in the service's promotional film.[164] "We're building trusted, consented, data sharing eco-systems that fill that void." The company is in a pilot stage and from 2008-2011 it worked to develop a secure digital infrastructure.[165] According to Vervenne[166], it's ramping up to deliver an individual cloud-based PDS that will ensure user privacy in data sharing processes and analyses.

163. StJohn Deakins, August, 2016, personal interview.

164. synergetics.be, 2016.

165. tas3.eu, 2015.

166. Luk Vervenne, February 2016, personal interview.

> **Meeco.me.** 'The Person is the Platform' is the mantra of Australian Katryna Dow, who is selling individual data control with her start-up Meeco.me. Here you can securely store and encrypt all your different personal data and you can learn to use it on various apps developed in the start-up's living lab. "There is no reason why we all cannot have our own API and create the same value with our data without the silos we are seeing today. We are moving away from being sold things to being involved in things," Dow said.[167]

All of these new services and companies (many of them are also in the US, such as Datacoup, Datawallet and Personal Black Box) offering individuals different types of control over who sees their data, what they see and when, indicate a general trend towards empowering people in daily data exchanges between each other, businesses and public authorities.

TRADITIONAL PLAYERS GO 'MY DATA'

Start-ups aren't the only ones to join the My Data movement. In Italy and especially France, we're seeing traditional players head down a more individual-empowered route. They're increasingly developing new services where users get access to and gain ownership of their own data – not least get a better understanding of their data.

> **Telecom Italia.** This southern European telephone provider has introduced a service called My Data Store, where its customers can collect all their data – from location and expenses to social media and detailed retail info – and keep it in a secure personal data cloud. They then have control over whom they share data with, when and for how long.[168] With this service,

167. Katryna Dow, September 2016, personal interview.

168. My Data Store: a Personal Data Store concept by SKIL Lab, 2016.

based on Privacy by Design principles according to the company, customers can also get to know themselves better by using their own data in various apps, such as a personal money manager and tools supporting their purchases. Telecom Italia also built some services in the smart city of Trento based on the data storage platform allowing consumers to have more control.

AXA. The French insurance company with 100 million plus customers in over 60 countries is one of the first-movers among larger players to incorporate a more human centric approach. Not only was it the first insurance group to have approved Binding Corporate Rules and set up data privacy compliance teams at Group and local levels), they also have customer commitments where they explain why and how they use data. For instance, They have taken the decision at group level never to sell the personal data of their customers. Axa also has a Data Privacy Advisory Panel whom they fly to Paris two to three times a year to proffer up food for thought on new issues arising in the wake of technological advances. Lastly, the insurance group also spearheads AXA Research Fund supporting research initiatives to better understand the issues at stake around risks in general. This includes a new area of funding around big data and data privacy.

Both Telecom Italia and AXA are making efforts to provide their customers with access to and insights on their own data because they believe it will enchance and conserve their customers' digital trust. At the same time, it will give them more accurate and varied data in order to devise and offer better products and services. AXA is also – with explicit informed consent – enriching some customers' data with that from social media. "Before we did all this, we had offered our customers a bracelet to measure their exercise, but it was not a success. So

we stopped this experiment, as our customers were not adhering to the concept," said Cecile Wendling[169], head of foresight at AXA.

According to the Senior Officer in the Strategy and Innovation Department of Telecom Italia Michele Vescovi[170], experiments up to now have shown that people tend to share more data when they understand and control it, and when they can use it to gain direct benefits, such as saving time and money or generating social value.

RISKS ARE LINING UP

The interests, objectives and actual solutions within PDSs and My Data differ greatly and there are benefits and pitfalls to all of them. With commercial offerings, undoubtedly the user will gain better insight into his/her digital self and behaviour, and there is the potential to shift the balance towards empowering the individual in decisions about what is 'appropriate' for him/her, rather than being dictated by a company's proprietary algorithms. Making money on one's own data is probably not something one should expect to be lucrative, since it's really copious amounts of data that create wealth. But at least the individual has the chance to become part of a more equitable business model.

At the same time, there is an embedded ethical problem in models that describe personal data as currency and profit. Are we in the process of creating a digital divide, where those who can afford it have privacy and a private life, while the economically vulnerable groups in society will be forced to sell theirs?

With the Personal Data Store trend comes other risks also. The most effective way individuals protect their data and privacy online is by, among other things, spreading their data and using many different identities. A PDS typically gathers all your data in one place (some of them even let you decide where to store it). This is unsafe in and of

169. Cecile Wending, September 2016, personal interview.

170. Michele Vescovi, September, 2016, personal interview.

itself, because no one can guarantee secure data storage. Therefore, niche PDSs, where you can spread your data over several different locations, are perhaps a better solution. Moreover, it's an enormous responsibility to put on the shoulders of individuals who would have to familiarise themselves with their own data – let alone control it.

Moving forward, PDSs will have to be extremely user-friendly. No matter what happens, any PDSs that manage to build confidence based on credible technical and organisational approaches and expertise may come to play an important role as the independent third parties that we leave personal data control to.

But first, many PDS providers will need to demonstrate that they are actually trustworthy. Mydex in England is trying to do this with an ISO-certification, but there will also be other accreditation schemes, such as the upcoming EU privacy seal, expected to be established in the wake of the new EU data protection regulation.

A French NGO, Fing, has been leading a group of experts under the name MesInfos to develop a set of PDS guidelines – a Self Data Charter, as they call it. Those who sign the Charter commit to complying with European data protection legislation, to working for individual autonomy, and allowing individuals to fully dispose of their own data as they please.

MY DATA INFRASTRUCTURE

The hypothetical constellation of new PDS providers will need to communicate with each other and thus standards will need to be developed to share and exchange data across platforms. One of the key challenges is that these different systems don't necessarily talk to each other yet, making it difficult to move data or convey it across services. However, there are several ongoing initiatives designed specifically to create a new type of infrastructure.

Mydata. The Finnish government is backing an ambitious project to create a new, digital, personal data infrastructure,

Mydata.[171]They call it a human centred approach. With its open source infrastructure, individuals and organisations can be My Data administrators and manage accounts for others. But it's also possible to host one's own account, just like it's possible to host your own email server at home. Mydata is not a PDS or personal cloud account which offers the secure storage of personal data. Rather, its main objective is to ensure a structure for consent across services. With open APIs, users can get a dashboard to grant or withdraw consent, and anyone with access to their data can tap into it via the open Mydata API.

Hub of All Things. In the UK, seven universities are cooperating to create a new breed of infrastructure. On the platform called HAT, you can trade and share personal data in a standardised, structured way. Individuals can gather their personal data on the platform via a HAT-operator, whom they choose themselves, in the same way that we can choose between different email providers. Individuals can use the platform to gain more insight into their own data to then share or sell it, and to personalise the services they consider relevant. Companies can also use the platform to provide customised offers.

Personal data in blockchain. A group of researchers are creating a type of PDS service without having a third party, business and/or organisation, in control of the data on behalf of others. To the contrary, they believe that blockchain technologies can give each and every person the ability to control his/her own data.[172] There are three types of stakeholders: users of smart phones, services for smartphones,

171. MyData – A Nordic Model for human-centered personal data management and processing, 2015.

172. Decentralizing Privacy: Using Blockchain to Protect Personal Data, Guy Zyskind, Oz Nathan, Alex Pentland "Sandy", MIT Media Lab, 2015.

> and 'nodes', the many decentralised units that control, one by one and together, the blockchain infrastructure. The researchers, hailing from Israel University and Boston's MIT, don't think that personal data should be handled by third parties, as it's a vulnerable and uncertain system. They believe primary control should only lie in the hands of individuals. Blockchain technology, they argue, ensures this, and makes sure that companies getting access to data can focus on using it (rather than protecting and securing it). It will also become easier to enforce data protection legislation, as it will be programmed directly into the technology and enforced automatically.

If the Personal Data Stores take off, then – in order to be successful – individuals will need to take responsibility for and care about their own data. Not many will jump on the bandwagon immediately, and there will be a need for credible organisations to act as middlemen for those who won't do it on their own. At least until operating one's own Personal Data Store is as easy as opening an Instagram account.

Privacy is control over one's data and the right to decide who knows what about you and when.

CHAPTER 13

WHAT IS PRIVACY?

Privacy is like trust and security; much easier to define when you don't have it. We know exactly what trust and security are when we find ourselves in a precarious situation where we feel threatened, a situation which reveals someone else's lie or dishonest actions. It's something that can make us feel angry, insecure and most importantly, disempowered. The same is true of privacy; it's hard to put a finger on it before we realise it's missing. More and more of us are beginning to sense the lack of privacy in our digital daily lives – and to understand what we are missing and how we feel about it.

Data ethics is first and foremost about balancing the powers embedded in society. Individual privacy is not the only societal value under pressure in the current data-saturated infrastructure. The effects of data practices without ethics can be manifold – unjust treatment, discrimination and unequal opportunities. But privacy is at its core. It's the needle on the gauge of society's power balance.

In a well-functioning democracy, those in power are open and transparent about how they exercise their power. One should not expect transparency from individuals. The more transparent people are, the more vulnerable they become.

With the current digital infrastructure we are heading in the wrong direction: individuals are becoming more and more transparent, open to different types of control, manipulation and discrimination, while the powerful – government, industry and organisations – are more and more closed off. Freedom, individual independence and democracy are fundamental reasons why the individual right to privacy is something we should all care about.

Privacy is a universal human right penned in international conventions, declarations and charters which were formalised at a time in history when private life was the default. There were clear lines and limits between private homes and public streets and buildings, between a private person and the public authorities and spaces. It was the letter in the sealed envelope. But the digital media's foothold in the world has, as Professor Joshua Meyrowitz illustrated in 1986 in his book *No Sense of Place,* slowly but steadily been breaking down walls between public and private. First when radio and television brought the public sphere into the private living room, and later when the Internet and mobile phones allowed us to literally feel public life vibrating silently in our pockets. Machines started going through our private emails and conversations. The envelope was opened. We increasingly unfold our identities, our lives, in online social networking spaces and privacy is something we must actively opt in to. At the same time, these online spaces create our identities; they limit us or create opportunities and privacy becomes a tool of empowerment.

In reality, privacy *is* empowerment. The fact that we actively use digital media and share details about ourselves does not mean that private life has no value, that it's no longer a social norm as Facebook's Mark Zuckerberg was once quoted as saying.[173] It just means that privacy has new conditions. To have a private life, an image, or an identity online is about empowerment. Empowerment means you can decide who knows what about you and when – now and in the future

173. Privacy no longer a social norm, says Facebook founder, The Guardian, 2010.

– and that you can exercise control over the outcomes springing from this knowledge.

Privacy is a characteristic unique to the individual. What we choose to disclose or not disclose, and in which contexts, is deeply personal and distinctive to us as separate entities. Privacy is unique to cultures and individuals and, exactly for this reason, it matters. It empowers each of us to act in our own specific capacity.

Privacy is an everyday social practice. Google's chairman, Eric Schmidt, has said that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[174] According to this logic, privacy is only about the secrets, the sultry or even criminal details. But if we turn this logic around and look at what we are missing if we do not have a private life or do not have the basic features that make privacy possible, the argument fades. In a tangible world parallel, we get up every morning and cover our bodies with clothes and close the door to go to the toilet, yet no one would argue we are doing something we shouldn't. Our everyday practices are in themselves proof that privacy is a principle that allows us to act as independent individuals in a social space.

Privacy is a democratic value. It is free thought and independence. Studies show that people change their behaviour when they feel watched. They seek information less freely, act and express themselves less freely, are afraid to stand out and go against the flow.[175] Trevor Hughes, CEO of the International Association of Privacy Professionals, IAPP, has a good explanation of the importance of privacy: "As humans, we seek solitude when we feel vulnerable. Sometimes, this is related to physical vulnerability. We seek to exclude ourselves from our societies when we are sick, or in moments of particular risk (think: sleeping, toileting, sex, etc.). But we also seek to exclude

174. Inside the Mind of Google, CNBC, 2009.

175. Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring**,** Elizabeth Stoycheff, Journalism & Mass Communication Quarterly, March 2016.

ourselves when we feel emotionally vulnerable. We seek private space to explore new identities or ideas."[176] Privacy and the space to think and act without feeling watched is a prerequisite for individuals' ability to act independently and freely. A private life ensures that each person can create his or her own unique identity and determine his or her life's direction - the right to fail along the way or to go against the tide. The right to privacy is thus a prerequisite for active democracy.

And last but certainly not least, privacy is the prerequisite for free innovation and creativity. As law professor Julie E. Cohen put it: "Innovation requires room to tinker, and therefore thrives most fully in an environment that values and preserves spaces for tinkering."[177]

176. Keeping humanity in the privacy debate, CSO, 2016.

177. What Privacy is For, Julie E. Cohen, Harvard Law Review, Vol. 126, 2013.

Data ethics is more than just compliance with data protection regulations.

CONCLUSION

THE DATA ETHICAL AGENDA

We need ethics to survive in the data era. While new technologies and data innovation move full steam ahead, we're only beginning to grasp the transforming power of this evolution – how it is transforming our daily lives as well as social and global dynamics.

Today, companies have cookie policies, privacy policies, data management policies and user terms of conditions for their data. But they need more than that. Legal terms are one thing, common sense is another.

Technology shows us what we could possibly do with data.
Laws and regulations show us what we're allowed to do.
Ethics tells us what we should do.

An ethical system is not neutral, neither are laws and technology. Data ethics is the moral management of the human repercussions stemming from digital data developments. With ethics, we determine the 'right' and 'wrong' with an eye towards shared cultural value systems and social agreements.

Digital ethics, and in particular data ethics, is beginning to take up more and more of the public debate on digital tech's influence on society, economy and culture. Based on the realisation that laws have not kept up with digital progress, technologists, academics, policymakers

and businesses are revisiting cultural values and moral systems as they search for a new ethical framework for the digital age.

Law is designed, among other things, to protect individuals from discrimination, unfairness and exclusion and to ensure fair market conditions for businesses. But laws also include interpretations and exceptions, and legal grey areas created by the fast pace of technology will create margins that may not always be in the individual's, or for that matter the fair market's, best interest. Informed regulation is necessary, but it isn't the answer to all ethical dilemmas. The data-ethical companies are the ones that do more than simply comply with data protection legislation. They also uphold data-related ethics and values.

We are living in an age of experimentation where laws, technology and our limits as individuals are tested and negotiated on a daily basis. We see changes in legislation, national and international governance and citizen awareness, and the sum of all these efforts will pave the way into a responsible technological future – one that includes the ethical treatment of data.

This book is primarily focused on the private sector. Though the current data-driven, tracking-by-default infrastructure was first and foremost created within this sector, we are beginning to see positive, constructive action. Many companies are experimenting with new business models, technologies and organisational formats that put the empowered individual at the centre. As we argue, this is primarily because data ethics is becoming a part of a sustainable, trust-based data economy.

The elite will spearhead a new market for privacy tech just as we have seen it with green tech.

In the beginning, privacy will be for the elite. It will be the highly educated, well-off, well-known and powerful that will pay for their privacy and data control, because they either need it more urgently or

simply because they can – be it tools helping them protect their personal data or services giving them control over that data.

Individuals, however, are not alone in the responsibility to preserve the right to privacy. Governments and companies are also. The responsibility is, in fact, three-fold. And while laws and business practices, common international standards and cultural frameworks are negotiated, the most resourceful individuals will surely take action.

With past environmental challenges, we saw the emergence of new environmental business requirements and a market for green products. With big data challenges, we will see the emergence of a formal framework for data-ethical business practices along with this new market for privacy tech. As the demand for individual data control increases, prices will go down and more people will gain access to such products and services. But before this can happen, we need a regulated market economy to foster these changes.

To create a common approach and understanding of the challenges and solutions we describe in this book, it's necessary for all to participate: developers and regulators, computer scientists and designers, scientists and philosophers, but especially ordinary people. Consumers must demand their rights to control their own data. After all, the creation of a sustainable infrastructure for the data era is not just a business or technical project, not just a legislative, social or economic objective. And it certainly isn't something anyone can do alone.

We would like to extend a special thank you to:
Flemming Muus
Clara

And an additional thanks for their helpful review of various chapters:
Marianne Steen, Birgitte Kofod Olsen, Rikke Frank Jørgensen, Martin Glarvig, Robin Wilton.

APPENDIX

THE DATA ETHICAL STRATEGY

For inspiration, below is a list of areas to be considered for a data ethics strategy. The list is not exhaustive as there are a number of overarching strategic, organisational and technical decisions that need to be in place when working with data ethically. Furthermore, a list of concrete alternative tools and services that companies or organisations can use when working with data ethics can be found here: **dataethics.eu/tools**

DATA MINIMISATION

Not all data is good data or useful data. Collecting unnecessary troves of data is a risk for the company and the customers. Be conscious and reflect on what is processed, where and how data is stored, and give the customers control over their data.

ANONYMISATION

Anonymisation of personal data by encryption (see also below) or removing personally identifiable information from data sets is a must. But it's important to remember that anonymisation is not an easy way out. There is always an embedded risk in the collection, storage and processing of personal data. Even when anonymised, the possibility of

identifying individuals still technically exist if the data set is large enough also encrypted communications' meta data may also be very revealing. Some data which is not personal per se can become so when correlated with other types of information. On this topic, Apple's bet on 'differential privacy' is a concept to explore.

ENCRYPTION OF COMMUNICATION

Companies might include services where customers need to communicate with a company, organisation or other customers. One thing is to encrypt data traffic, so that potential eavesdroppers cannot capture data while in transit, another is end-to-end encryption meaning that not even the service provider (the company) can get access to that communication either. Using end-to-end encryption has become a major privacy selling point of big communication services.

TRUE TRANSPARENCY

Is your company truly transparent? Does it show how it collects, verifies and processes customer data? To be open and honest about use of data can foster customer trust – and even make customers more willing to share their data – as well as prevent abuses of power.[178] Apart from having a clear and understandable privacy policy on the website, companies can do a number of other things to tell their customers about the way they process and protect data. For example, does your business have good marks in initiatives that rank companies by their human rights and privacy policies, such as Ranking Digital Human Rights? Companies can also tell their customers directly how they make money. When your enterprise doesn't capitalise mainly on data, but off hardware or specific products, it's a good idea to differentiate from other companies that provide the same service by informing your customers about your data privacy policy. If your company doesn't

178. Big Data Ethics, Richards, Neil M. and King, Jonathan H., Wake Forest Law Review, 2014

give its product away for 'free', it's a good idea to explain why it costs money to use your service. Businesses can also make a video to explain the company's approach to data.

KNOW YOUR CUSTOMER

How well do you know your customers? It's one thing to look at general surveys on consumer behaviour, it's another to actually ask customers and potential customers directly in order to get a better sense of how they feel about the data you hold or want to hold on them. How far can you go before you cross their creepiness line? Asking and listening to your customers will also help them understand that you take their data privacy seriously.

SUBCONTRACTORS

If a company takes responsibility for its subcontractors when it comes to the environment and working conditions, why not also in terms of how it treats customer data? What are the data protection standards and ethical practices of the partners that store, process and analyse your customers' data? Do they repurpose that data? Do they sell it? What are the laws (and the jurisdiction) applied to them? Are the legal requirements and frameworks comparable to the ones your business operates within?

COOKIES

Cookies can benefit a company when they provide insights into customer behaviour. But third-party cookies – or marketing cookies – can also send your customers' data and behaviour into the hands of your competitors. Businesses and organisations should continually check their websites for unwanted cookies or other trackers. Ask yourself if you really need marketing cookies. First-party cookies are fine, as they don't share data with others and help customers remember passwords

and what they put in their shopping basket. A company with no ads on its website could relatively easy decide to remove all third-party cookies, and in some European countries (such as Holland) you don't even have to show a cookie-policy warning if you only use first-party cookies.

SOCIAL PLUGINS

One category of third-party cookies comes from companies like Facebook, Twitter, Google Plus and other social media. So-called 'social plugins' are used on news sites, for example, to share content and log in via a user's social networking accounts. They're a potential risk, because the social buttons and the content they pick up are stored on the social media site's own servers. They may make it easier for users to share content from the website, but they're also a powerful tool used by Facebook, Twitter and Google to track a site's customers and their behaviour (even if they don't click on the buttons).[179]

ANALYTICAL TOOLS

Google Analytics, which a majority of websites use to analyse traffic, is 'free' for companies. Instead of sending money the website pays with data. Through its Analytics program, Google harvests in-depth knowledge about a company's websites users – and customers. To use Google Analytics in Germany, a website is required to anonymise all IP addresses, and the end user must be provided with an easy way to opt out of any Google cookies. The website is also required to institute a data processing agreement which specifies that Google can solely treat the data according to the customer's instructions. For German authorities, it's not legal to unconditionally, continuously track users on a public website. There are a number of good alternatives to Google Analytics.

179. Changes to the Blog, Schneier Blog, 2013.

DATA STORAGE

In the wake of Edward Snowden's surveillance revelations, a number of European cloud service providers have succeeded in promoting themselves on the fact that all their data is stored on servers physically located in Europe. Cloud service customers have become concerned with the risk of industrial espionage and other unauthorised access to their data – including intelligence services in the United States as well as other countries – that could pass on their knowledge to national competitors. Some countries, Russia and Brazil for example, are quite strict about having data on stored on physical addresses in within their borders.

SEARCH ENGINES

Google's search engine has become the standard on browsers and computers worldwide. Google Search personalises search results by tracking and creating a profile of each user. Today, there's a wide range of alternatives that are not based on tracking. Any data-ethical business or organisation should decide which default search engine they will use and what implications this setting will have in relation to its data ethics policy.

CONSENT

Even if a company has obtained a user's consent to a service, it's not guaranteed that the user actually understands what s/he has agreed to. And when that same person later experiences the use of his/her data directly, it may have a negative impact on the trust relationship with the company. In the EU data protection regulation, there's a clear requirement that consent must be specific, informed and relevant.

PRIVACY POLICY

A data-ethical privacy policy should be easy to understand, honest, descriptive and available in a few versions: one for those who do not bother to read lengthy explanations and another for those who do – including lawyers and privacy experts. It uses a clear language to explain why they need or do not need data, how it's deleted, how you can request it, and that access to their data is not sold to third parties. Some go a little further with their privacy policy by also providing a customer privacy promise/pledge. Many companies would be wise to include statements about what will happen to customer data if it were to go bankrupt or be sold.

INTERNAL COMMUNICATION

It's equally as important for a company to communicate its data ethics internally. Its employees' sense of ownership over a data ethics strategy, and their behaviour in relation to data in particular, is pivotal. Uber, for example, lost a good deal of credibility when it emerged that employees had access to the system and could follow cars and named customers around via the dashboard. One of the employees couldn't resist contacting one of the customers[180] in a car in New York, an event which was talked about all around the world, branding Uber as a company that's careless with customer information. Employees need to know that respectful treatment of customer data is paramount. It's also vital for only a minority of employees to have access to the parts of customer data they crucially depend on according to their role.

180. Can We Trust Uber?, Silicon Guild, 2014

EMPLOYEE DATA

The company's own processing of employee data can also be included in a data ethics strategy. For example, it may be legal for a company to monitor its employees' emails, but is it ethically justifiable?

PRIVACY SEALS

A product or service can get a privacy certification. In the wake of the new EU Data Protection Regulation, we'll see privacy certifications which are quite similar to current environmental certifications.[181] Until they've been launched there are a range of certifications that are already on the market. There's the German/European Europrise, which was originally founded by one of the German data authorities, but now is privatised and based on strict criteria. The UK Data Protection Authority ICO plans to launch its own privacy certification and there are a number of other private (albeit less reliable) certifications, including the US-based Trustee.

181. EU Privacy Seals Project, 2013.

SELECTED LITERATURE & REPORTS

Big Data Ethics, Neil M. Richards, Jonathan H. King, Wake Forest Law Review, 2014

Big Data: A Revolution That Will Transform How We Live, Work, and Think, Viktor Mayer-Schonberger, Kenneth Cukier, John Murray Publishers, 2013

Blockchain Revolution, How the Technology behind Bitcoin is Changing Money, Business and the World, Don Tapscott, Alex Tapscott, 2016

Data Brokers: A Call for Transparency and Accountability, Edith Ramirez, Julie Brill, Maureen K. Ohlhausen, Joshua D. Wright, Terrell McSweeny, Federal Trade Commission, 2014

No Place to Hide, Robert O'Harrow, Free Press, 2005

Obfuscation, **A Users Guide for Privacy and Protest**, Finn Brunton, Helen Nissenbaum, MIT Press, 2015

Privacy on The Ground, Kenneth A. Bamberger, Deirdre K. Mulligan, MIT Press, 2015

Personal Data Stores, Guillaume Brochot, Julianna Brunini, Franco Eisma, Rebekah Lasen, Daniel J. Lewis, Dr. Jin Zhang, Cambridge University Judge Business School, 2015

Risk Society: Towards a New Modernity, Ulrich Beck, Sage, 1992

Taking Trust Seriously in Privacy Law, Neil M. Richards, Woodrow Hartzog, Stanford Technology Law Review, 2015

Terms of Service Social Media and the Price of Constant Connection, Jacob Silverman, Harper Collins, 2015

The Black Box Society - The Secret Algorithms That Control Money and Information, Frank Pasquale, Harvard University Press, 2015

The Future of the Internet - And How to Stop It, Jonathan L. Zittrain, Yale University Press & Penguin UK, 2008

The Individual and Privacy, Vol 1, ed. by Joe Cannataci, Routledge, 2015

The Internet of Things: Mapping the Value Beyond the Hype, James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, Dan Aharon, McKinsey Global Institute, 2015

The Fourth Industrial Revolution, Klaus Schwab, World Economic Forum, 2016

The Privacy Engineers' Manifesto - Getting from Policy to Code to QA to Value, Michelle Finneran Dennedy, Jonathan Fox, Thomas R. Finneran, 2014

The Reputation Economy, Michael Fertik, piatkus, 2015

The Secrets of Surveillance Capitalism, Shoshana Zuboff, Frankfurter Allgemeine, 2016

Trusting Big Data Research, Neil M. Richards and Woodrow Hartzog, Stanford Technology Law Review, 2016

Understanding Privacy, Daniel Solove, George Washington University Law School, 2008

Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring, Elizabeth Stoycheff, Journalism & Mass Communication Quarterly March 8, 2016

What Privacy is For, Julie E. Cohen, Harvard Law Review, Vol. 126, 2013

Why Youth (Heart)Social Network Sites: The Role of Networked Publics in Teenage Social Life Danah Boyd, in MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume (ed. David Buckingham). Cambridge, MA: MIT Pres, 2008

KEYWORDS

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z

Ä