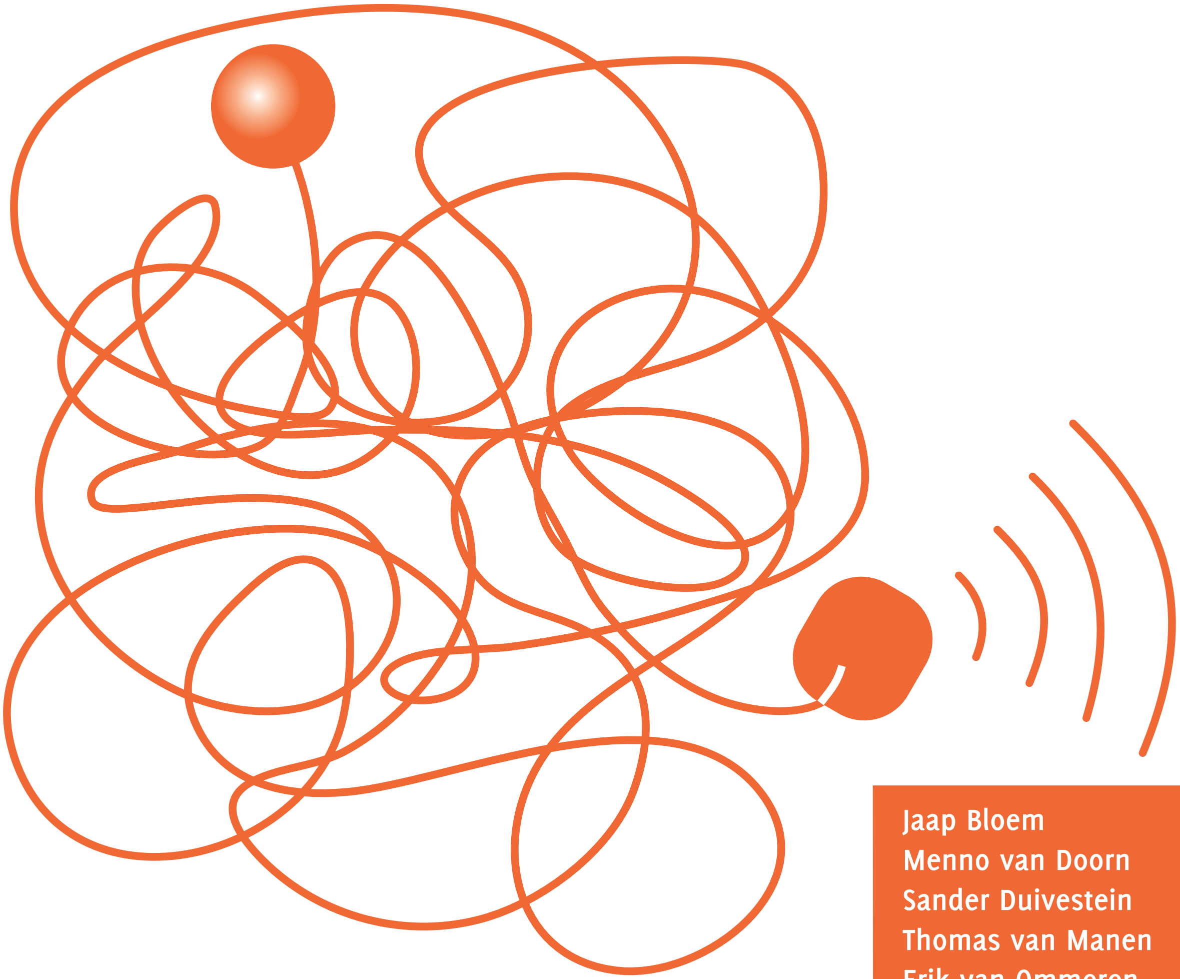
VINT research report ① of 4
VINT research report ② of 4
VINT research report ③ of 4
VINT research report ④ of 4

Privacy, technology and the law

Big Data for everyone through good design



Jaap Bloem
Menno van Doorn
Sander Duivestein
Thomas van Manen
Erik van Ommeren

SOGETI

VINT | Vision • Inspiration • Navigation • Trends

vint.sogeti.com/bigdata
vint@sogeti.nl

Table of contents

The VINT Big Data research reports 3

Introduction
Reaping the fruits of Big Data

1 An anatomy of Big Data anxiety 9

2 What is privacy? 21

3 Privacy by Design and the balance between PITs and PETs 36

4 Legislation in a state of flux 44

Conclusion 51

Literature and illustrations 55

Privacy: great – but what's the next step…? 62, 64

About Sogeti 63

About VINT 63

For informational use only. This publication has been compiled with the greatest possible care, but no rights may be derived from its contents.

© 2013 The Sogeti Trend Lab VINT | Vision • Inspiration • Navigation • Trends
Book production LINE UP boek en media bv, Groningen

SOGETI

VINT | Vision • Inspiration • Navigation • Trends

The VINT Big Data research reports

Since 2005, when the “Big Data” concept was launched – remarkably enough by O’Reilly Media, which had introduced Web 2.0 only a year earlier – Big Data has become an increasingly topical subject. In terms of technology development and business adoption, the Big Data field has undergone extremely rapid changes. And that is an understatement.

In *Creating Clarity with Big Data*, the first of a total of four research reports, we offered an answer to questions about what Big Data actually is, where it differs from existing data classification, and how the transformative potential of Big Data can be estimated.

The concrete adoption and plans of organizations are currently and primarily oriented toward the theme of our second report, *Big Social:* basically the customer side, particularly inspired by the social network activity of Web 2.0.

The data explosion is taking place all around us, but a major part of the discussion concerns the extent to which organizations should now plunge into Big Data. The answer is: only on the basis of a well-grounded policy. Such a policy – external as well as internal – is central to privacy issues, which will be comprehensively covered in this third research report.

When privacy in a digital context is examined, it is inevitably bracketed together with the protection of personal data (data protection, *Datenschutz, informatique et libertés*) and vice versa. We may wish to protect all the data in the world, but perhaps the best thing to do is simply to delete it. The DeleteMe app by Abine can be taken as an implementation of *The Right To Be Forgotten*, which the European Union, among others, propagates for our digital world.

To date, the differences in regions and countries all over the world are still great, but the harmonization and uniformization of legislation are increasingly being pursued. For all that, challenges are plentiful and technology is continuing to develop rapidly, particularly in the field of Big Data processing and analysis – see the VINT reports 1 and 2.

Top-down (through legislation) and bottom-up (through procedures and technology), efforts are currently being implemented with the aim of working toward one converging *Privacy by Design* solution. The idea is to provide a foundation for our information society from a social and economic point of view that respects the individual values and dignity that we cherish, all this with as few rules as possible and supported by the technology driving the change.

With four Big Data reports, VINT aims to create clarity by presenting experiences and visions in perspective: independently and furnished with appropriate examples. But not all answers, by far, can be given. In fact, more questions will arise: about the strategic choices you may wish to make, for example. We devote our fourth Big Data report to this subject. There may also be questions about how to restructure your organization. But to start with, this report goes more deeply into the privacy issues that Big Data analyses evoke.

We are only too pleased to exchange ideas and opinions with you about the new data focus: online at http://vint.sogeti.com/bigdata and, of course, in personal discussions. By actively participating in the discussion you will help yourself and us to further refine all concepts relevant to Big Data, with the ultimate aim of gaining progressive insight into taking clear and responsible decisions.

Join the conversation

In the context of inspiration, this report presents seven issues about which we would be glad to hear your views. The downloadable PDF document allows you to click on the relevant buttons. You will then switch directly to the relevant discussion. The answer to the key question "Privacy: great – but: what's the next step...?" is given on pages 62 and 64, the back of this Big Data report.

Introduction
Reaping the fruits of Big Data

Predicting and targeting as the Big Trick 4
Transparency, choice and Privacy by Design 5
Big Data gain for everyone 6
Big Data to become more privacy-friendly 7
The personal information economy 8

Predicting and targeting as the Big Trick

Data are the fuel of the digital economy. Everything that is possible nowadays may be extremely helpful and useful, but may also be threatening, or at any rate undesirable. The intelligence of a smartphone never goes amiss in the superstore when it comes to deciding what to buy for dinner, considering our dietary preferences. This is a wonderful thing of course, assuming that the collection and combination of data are dealt with transparently and discreetly. Quick digital advice supplied in this way, on the basis of preferences, is usually warmly welcomed. At one time Amazon started this in the retail business, to satisfy their customers and keep them satisfied as much as possible. The organization knows the customer and no one needs to feel cheated.

But in the case of the American Target chain – apropos of *targeting* – a clever analysis of purchasing behavior enabled predictions as to who was pregnant and also when the delivery was likely to take place. But Target was not transparent to the customer with respect to this kind of practice, and so it happened that the father of a teenager was unpleasantly surprised by the offers Target made to his daughter. True, Target was right and the girl had indeed been pregnant for as many weeks as they said, but it initiated an extensive discussion in the press about what organizations know about us and how they are using their Big Data knowledge to sell as much as possible.

Appropriate dead-on targeting is a wonderful thing, but we are rarely told what organizations know about us and how that knowledge is being used. For decades, this transparency has been a crucial part of the so-called *Fair Information Practice Principles* (FIPS, *Data Protection Principles* in Europe), but obviously some corners are being cut here. You may be familiar with the Target example from our previous research report *Big Social* and there are those who will make no issue of it; but what if your credit, mortgage or insurance application is rejected because the data indicate that your financial situation and/or health constitute an unacceptable risk to the provider? Which information is involved here? Where does it come from? How has it been collected? Do you have access to it? Can you change it? These simple and fundamental questions are a tricky problem in the age of digital information and have been for decades, in fact. Countless books have been written and there is much jurisdiction on the positively Kafka-esque examples of people who have come to be put in a bad light.

By and large, the major advantage of Big Data is its ability to make better predictions and selections. To organizations, the opportunities are ubiquitous: fraud detection, more efficient energy supply, offers tailored to the customer, anticipating epidemics, etc. One would expect that this would benefit all, but which data are being gathered by digital monitoring systems and what is being done with them? Do we have any idea about them and any control over them? The consumer/citizen, who is kept in the dark, often experiences this as one Big Trick. He or she feels that his/her privacy is being invaded – and so it is, of course. This third Big Data research report, *Privacy, technology and the law*, addresses that confrontation.

Transparency, choice and Privacy by Design

Where does this lead us? First and foremost to the conclusion that any organization engaged in Big Data should be thoroughly familiar with privacy and data protection. Evidently this is not always the case. If we are transparent and open about what we are doing, if customers are offered a clear choice whether or not to supply information and if we are implementing the *Privacy by Design* principle, the three most important steps have thus been taken. It is along these lines that this reports seeks to contribute to a fundamental privacy awareness that structures business activities in terms of transparent data management, which is for the benefit of customer and supplier alike.

There can be no two ways about it: whoever tries to find an on/off switch for privacy will never find it. It is much more important to choose the right direction, so as to exploit Big Data to its full advantage. What we should aim for is "Big Data gain for everyone." The best way to go about this is by recognizing the privacy issues, exposing them in detail and leading them in accepted directions in all candor.

Big Data gain for everyone

There is no more forceful way of putting it than Meglena Kuneva did: "Personal information is the new oil of the Internet and the new currency of the digital world." Ms Kuneva, EU Commissioner for consumer protection, said this during her keynote speech at a roundtable meeting on data collecting, targeting and profiling in Brussels in late March 2009. But broadly speaking, it is about digital data, online as well as offline.

Ms Kuneva outlined the situation as follows: "The boom in terms of volume of all the collected personal data and its use for commercial purposes is one of the most important and controversial issues in the rapidly changing world of digital communication."

Boom, volume, speed, economic value and various kinds of digital personal information: welcome to the Big Data era. When using these terms, we find that digital privacy is completely analogous to the concept of Big Data, which is defined as a combination of *Volume*, *Variety* and *Velocity*, supplemented by some with *Veracity* and *Value*. This is important and controversial: a godsend to customer service, but with all the usual challenges.

"The Internet," said Meglena Kuneva in 2009, "and the new generation of digital communication and digital platforms offer huge opportunities to consumers. In terms of choice, access and opportunity they are among the most empowering tools consumers ever had access to. [...] Obviously we want these new opportunities to evolve on a permanent basis and therefore we need to boost people's confidence, which will be conducive to their participation." Kuneva emphasized that "the Internet is largely an advertisement-driven service and is kept going by the development of marketing on the basis of profiles and personal data."

She added the following comment: "Over 80% of the young Internet users think that all kinds of personal data are being used and shared in one way or another without their permission, and actually this is true." When it comes to privacy protection, Ms

Kuneva feels that the sorely-needed solution is to be more transparent when it comes to collecting data. “Consumers need to be informed that their data are being bought and sold, and they ought to be offered the opportunity to supervise these activities themselves.”

These views are by no means new. We have known for some decades now that the privacy landscape is very much in the making, thanks to increasing digitalization. Concisely paraphrased, the introduction to the book *Technology and Privacy: The New Landscape* (1997) puts it as follows:

> *Digital privacy is the capacity to negotiate socio-economic relationships by controlling your own personal information. Rules and regulations, policies and technology increasingly structure people’s relationships with organizations and governments.*

There are huge differences in terms of privacy regulations both nationally and supranationally, but we all tend to agree on one thing: the enormous potential of the digital economy. It is extremely important to harmonize data protection and business interests, and lay down their interrelationships in the various legal systems in a coherent manner.

Big Data to become more privacy-friendly

Big Data is not privacy-friendly. In November 2012 Brendon Lynch, Chief Privacy Officer of Microsoft, emphasized this once again at the European Data Protection Congress of the International Association of Privacy Professionals (IAPP). Even when anonymization has taken place, certain core data have been deleted or data have been “scrambled,” it is still perfectly possible to link specific information unequivocally to an individual, to a computer or some other personal device on the basis of the links in different Big Data collections, online as well as offline.

To counteract this *linkability* and (re)identification, Microsoft has now operationalized a technological Privacy by Design solution – after years of development – that guarantees the quality of digital data for targeting by organizations, while making individual people untraceable with absolute certainty. In Big Data circles the method is known as *Differential Privacy*.

Target, for one, had never bothered about notice and consent, two important privacy principles, but Brendon Lynch asked himself: how can you expect everything that happens in a Big Data world to be reported in detail, and that explicit consent be asked? In the same way that the financial world has its flash transactions, our Big Data world is absolutely full of flash information.

Interestingly, a visionary historical quote on the American Privacy Rights Clearinghouse website makes unequivocally clear that Big Data recombination is at the heart of privacy concerns today. Back in 1977, ominously two hundred years after the first official copy of the Declaration of Independence was printed, the US Privacy Protection Study Commission already exposed the "real danger" to come in the following terms: "the erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable." The crucial difference is that in our Big Data age the number of record-keeping systems has exploded and they are huge instead of "small," as goes for the continuous monitoring and real-time analysis and recombination of XXL data streams containing Personally Identifiable Information. As stated in the Obama Government's Consumer Privacy Bill of Rights of 2012, consumer data privacy is the lubricant and fuel for the global digital economy. So let's keep the engine running! And, by the way, when personal data is fueling the economy, why not tax it, as was suggested in for instance France?

Join the conversation

PbD question 1
Have you ever had anything to do with privacy issues? The Privacy by Design (PbD) approach is expressly intended to prevent this.

http://bit.ly/vintR3Q1

The personal information economy

The so-called "personal information ecosystem" is described in the *Protecting Consumer Privacy in an Era of Rapid Change* report by the American Federal Trade Commission of March 2012. This document contains extensive recommendations to organizations and policy makers along the lines, successively, of Privacy by Design, simple choices for consumers and transparency. In the economic system, the individual is central and a wide variety of data is being collected about all of us. This is being done by media, government institutions, energy suppliers, airline companies, credit organizations, the retail sector, telecom companies, cable companies, insurers, banks, hospitals, doctors, drugstores, browsers, commercial websites and social networks. Information brokers, including credit companies and the advertising industry, use and combine these data and in this way they end up in banks, for example, or with marketers, media, authorities, legal organizations, individuals, upholders of justice and employers. It concerns online and offline data, originating from individuals, their computers or other devices. The only situation where the recommendations of the FTC report are not applicable is where an organization only collects privacy-neutral information of under 5,000 individuals a year, and does not share it with third parties in any way whatsoever.

It may remain a mathematical limit, but with the increasing demand for Privacy by Design, transparency, openness, notice, consent and more particularly the individual control of the information collected with regard to storage, processing, combining and dissemination will increasingly assume concrete shape. Organizations need to be aware of this and be ready. This means: gathering fundamental knowledge and organizing your operation accordingly. In this context, we hope to make a contribution through this report.

1 An anatomy of Big Data anxiety

1.1 Digital intangibles are terrifying 9
1.2 Internet and privacy are uneasy bedfellows 12
1.3 Reasonable anxiety 13
1.4 Fear, Uncertainty & Doubt 15
1.5 Privacy by Design as solution track 16
1.6 Our landscape of technology and privacy in a nutshell 18

1.1 Digital intangibles are terrifying

In the past few decades, what had been owned and physically possessed by people for thousands of years – the mine and thine, private behaviors and domains over which no one else had any say except when expressly invited – has now shifted to digital information: to all sorts of personal data in databases and our everyday activities and dealings on computers and online. In short, the concept of possession also covers our digital *Personally Identifiable Information* (PII), and the ownership, access, collection, storage, use and dissemination of this information.

The more digital data going around in all shapes and sizes, the greater the anxiety that, for one reason or another, this might result in a situation where far more private information becomes known than we would like. This may vary from video pictures, location-oriented information and social media to databases, surfing and purchasing behavior on the Internet, as well as the data that smart energy meters can collect nowadays. The possible linking of these and other data – in other words, actual Big Data use in all its aspects – is not yet transparent enough, and there is justifiable anxiety concerning the effective protection of information.

This is demonstrated by hackers and cyber criminals who manage, time and again, to penetrate into all sorts of digital systems – subsequently plundering bank accounts, reselling information, or simply putting it online so that everyone can access it.
The way in which the digital arms race between attackers and defenders is going to develop is largely occurring beyond our range. This, too, is cause for concern and, in the absence of facts and a sound risk assessment and considering the security leaks that keep on occurring, it continues to nourish anxiety and speculation.

With regard to privacy, "digital" has largely taken the place of "physical." We may put on as many dark glasses as we want, but our digital traces tell a great deal about us, and these traces are relatively easy to get hold of if you want to. That is the situation as we know it today, or at any rate, as it is perceived. And the various actual situations as well as their perception are ripe for clarification and improvement. An example...

In late November 2012, the Dutch TV program *De Wereld Draait Door* ("The World Is Turning Mad") called attention to the Electronic Health Record (EHR). After earlier opposition, this facility will be started up again in 2013 in the form of an opt-in arrangement called the Personal Health File, which means that people have to give their explicit permission to be included in the register.

Wilna Wind, director of the Dutch Patients' Consumer Federation, and Internet expert Alexander Klöpping were sitting opposite one another. Wind is a passionate advocate of the EHR, whereas Klöpping is vehemently opposed to it. He alarmed the audience with stories of his experiences with the hacker scene. At the end of the discussion, Matthijs van Nieuwkerk, the TV host, asked the audience who would still consider joining the EHR. No one raised his or her hand. Despite the new opt-in regulation, people are still quite apprehensive – not least because Ms Wind repeatedly assured the audience that EHR security would improve from a score of 4 ("unsatisfactory") to a score of 8 ("good") within six weeks, while everyone was fully aware that this discussion has been going on for years.

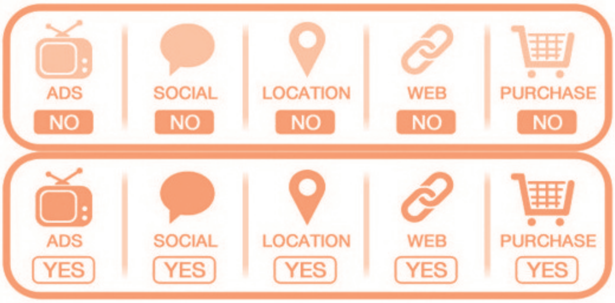
What can one conclude from this? Is Klöpping right? Evidently we hate to take the risk. To start with, weak spots in our privacy and data protection must be repaired as well as possible with the help of combined technology, procedures and regulation. We should aim for a so-called structural "Privacy by Design": privacy and data protection designed in conjunction with services and practices: an approach that is easily explained, offers optimum security, and inspires confidence.

Currently, specific fields of application for the Privacy by Design approach are the following so-called potential "Privacy-Invasive Technologies" (PITs). Obviously health care and Big Data Analytics are also included in the list:

1. Camera surveillance
2. Biometric recognition
3. Smart Meters and the Smart Grid
4. Mobile devices and communication
5. Near Field Communications (NFC)
6. RFID and sensors
7. Redesigning IP Geolocation Data
8. Remote Home Health Care
9. Big Data and Data Analytics

http://www.privacybydesign.ca

It is this trio of explanation, security and confidence, along with responsible behavior on the part of organizations and individuals, that will have to help us cope with our well-grounded – as well as irrational – fear of loss of privacy. When everyone understands the ins and outs of the matter and how the developments are likely to work out, this may form the basis for renewed consideration of a trade-off of personal data with an eye toward better individual service.



Fact and perception with regard to privacy can be communicated and addressed excellently through accreditations, quality labels and easy-to-read attachments. In 2012 the American Association for Competitive Technology, among others, made the set of pictograms shown below, which indicate what happens and does not happen with our personal data in the mobile apps that we download on our smartphones and tablets.

In America, the AppRights movement is working on a private member's bill, *The Application Privacy, Protection and Security (APPS) Act of 2013*, which is to regulate the collection of data via mobile devices and apps.

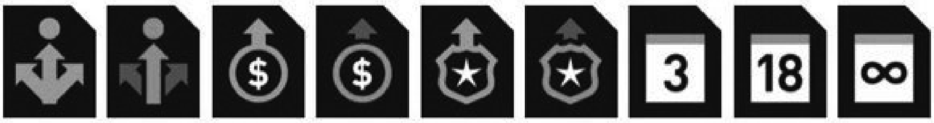
In September 2012, the U.S. Federal Trade Commission (FTC) already issued a clear set of guidelines for app developers called "Marketing Your Mobile App: Get It Right from the Start." Only to help them "comply with truth-in-advertising standards and basic privacy principles."

Fact is that many mobile app makers leave consumers confused or in the dark when it comes to app privacy options. Even worse, they deliberately mislead people, thus drowning the Golden Opportunity of monetizing Personally Identifiable Information in FUD: fear, uncertainty and doubt. Therefore, the FTC explicitely warns: "Laws that apply to established businesses apply to you, too, and violations can be costly."

To keep themselves out of trouble, app owners and marketeers should adhere to well-known Fair Information Practices regarding "Truthful Advertising" and "Privacy."

As from March 14, the European Union is moving in the same direction. The European data protection authorities, gathered together in the so-called "Article 29 Working Party," recently have detailed the specific obligations of app developers and all other parties involved in the development and distribution of apps under European data protection law. Other parties include app stores, advertising providers, Operating System and device manufacturers. Special attention again is being paid to apps targeting children.

This is happening more and more. Mozilla, among others, uses pictograms that indicate, for example, whether a website shares or sells data, passes them on to a government agency without a court order, and how long they are stored.



1.2 Internet and privacy are uneasy bedfellows

A survey among the American population of 1997, when about one quarter of all Americans were online, showed that, even then, people were extremely worried about Internet privacy. In the same year, the *Framework for Global Electronic Commerce* of the Clinton administration put it as follows:

> *Americans [and all other people] treasure privacy, linking it to our concept of personal freedom and well-being.* ***Unfortunately, the GII's [Global Information Infrastructure] great promise – that it facilitates the collection, re-use, and instantaneous transmission of information – can, if not managed carefully, diminish personal privacy.*** *It is essential, therefore, to assure personal privacy in the networked environment if people are to feel comfortable doing business.*

The Internet should not be a playground for undesirable and improper behavior, as this is detrimental to economic potential, or so it was argued. This results in a lack of confidence, causing customers and providers to stay away and preventing the free world market from developing as it should.

We are eager to allow the social and economic potential of the Internet to flourish as an everyday part of our lives. But its openness and speed carries a huge inherent risk of misuse. All stakeholders involved must accept responsibility here, ideally with the private sector taking the lead, as it has the greatest economic interest.

In 1997, people expected more and more individuals and organizations to actively use the Internet if their privacy could be fully guaranteed. But despite all such privacy concerns, the Internet continued to boom – so saying and doing are apparently two different things. Therefore, may the Dutch be expected to join the new EHR in due course, in spite of all their present skepticism?

To what extent is the fear of an EHR and other Big Data initiatives realistic? How easy is it to turn a score of 4 for security into an 8? Perhaps that is not hard at all and after all, people's reaction to change is often based on gut feelings.

The issue of whether or not current emotion and misgivings with regard to personal data will eventually wane again requires further analysis. The EU, at any rate, feels that generally speaking online privacy is not properly regulated:

Internet privacy is not properly protected. This is the view of the European Commission, which has drawn up new rules. However, these may not come into effect until 2015. In advance of this, Dutch regulations will be tightened *considerably as of this year. As they should, because the present law dates from 1995 and is hopelessly out of date. The major changes are:*

- *Data of consumers must not be used without their explicit permission.*
- *Companies have to outline their privacy policy in plain terms.*
- *Consumers are given the so-called "right to be forgotten."*

Companies not complying with the rules risk fines of up to 2% of the turnover, which for large businesses may amount to tens or even hundreds of millions of Euros.

RTL Z, 14 January 2013

It is the intention to ratify the so-called "General Data Protection Regulation" in the European Parliament in 2015. We are no longer talking about a guideline for national legislation, but a new European "act." This means that data-processing organizations will have to meet stringent requirements. Fines for businesses may run to 2% of the turnover.

1.3 Reasonable anxiety

Anyone compiling an anatomy of fear of Big Data will find that this anxiety is well grounded. In the previous century, the first Big Data factories, the credit-rating companies, followed rather dubious practices. They disregarded the law, made few or no rectifications of mistakes in data, combined all sorts of databases in a creative fashion in order to gather as much personal information as possible, and were constantly involved in court cases and hearings due to their procedures. In 2004 Robert Ellis Smith published a retrospective on the subject entitled *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet.*

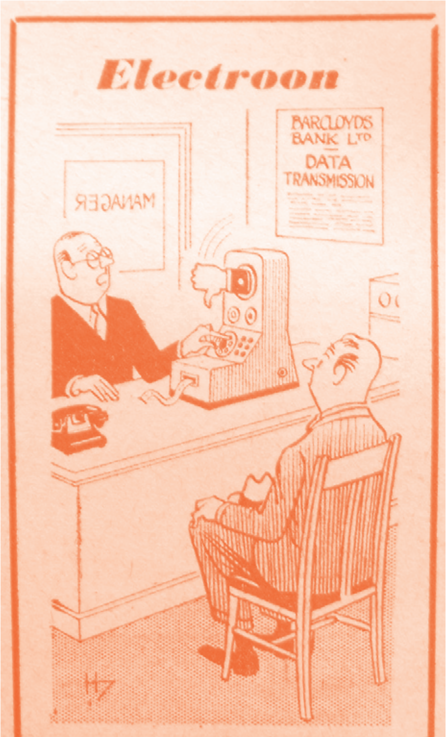
American credit-rating agencies such as Equifax, Experian and TransUnion combined citizens' personal data from a variety of databases, linked them with social security numbers, and subsequently used and sold those profiles. These credit-rating companies furnished information to banks and authorities that had to make decisions with regard to car loans, life insurances or benefits. According to Robert Ellis Smith, they also resold the information.

A negative credit assessment might ruin you. This is what happened to Keith and Phyllis Mirocha, who were not given a mortgage for their new home although they were clearly the victims of mistaken identity. With all the goings on and the legal battle they had to enter into – with TransUnion, in this case – the couple lost their jobs into the bargain.

The Mirocha case has many elements that nourish the Big Data anxiety even today:

- an unequal fight: large institutions versus the common man
- information is used without permission
- systems are making decisions without human intermediary.

It is quite a job to be proved right in this type of case. Even after the mistake in the file of the Mirochas had been detected and Trans Union had promised to correct the data, they were still refused a mortgage. The problem was that the wrong information was still in the system, and this barred the loan. It was a disagreeable situation that looked like something that had emerged from the hilarious "Computer Says No" sketch from the BBC series *Little Britain*. The following cartoon from *Electronics Weekly* of 2 November 1960 shows that this situation has a long history. Note the thumbs-down signal so emblematic of Facebook nowadays. It almost looks like a reference to the plan of Schufa, the German credit-rating agency, to link personal information from Twitter, Facebook and LinkedIn to their 66-million-customer database for the sake of better credit profiles.



"I'm sorry, Mr. Bagshawe, but it appears you are overdrawn already."

Two specific Big Data-related developments can be added to the three anxieties from the days of the Mirochas:

- Digital data reach other parts of the world in no time at all. Possible privacy invasion by America, in particular, are anathema to the Europeans.
- Personal information shared by people on social media threatens to be used against them by governmental authorities, insurers and other organizations.

The "Computer Says No" syndrome has remained a controversial issue to date. This is clearly illustrated by the first *Issues Paper* published by the South Australian Law Reform Institute of Adelaide University Law School in May 2012. Its title is: "Computer says no: Modernisation of South Australian evidence law to deal with new technologies."

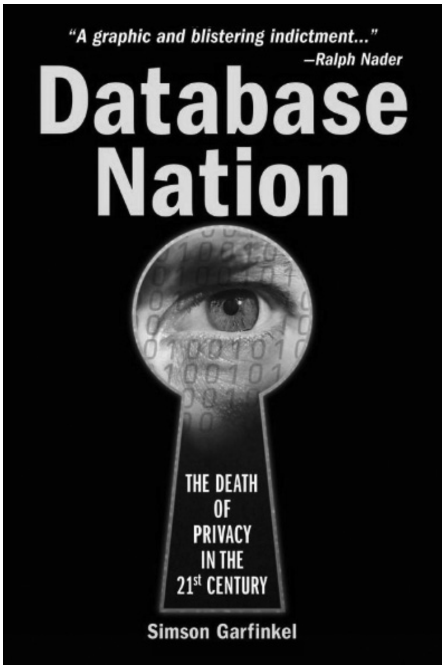
The story of the Mirochas is illustrative of what was going on at Equifax on a large scale. During a hearing it turned out that employees had been pressured to obtain a certain quota of negative reports on consumers. This put them up to fabricating data in creative ways.

Equifax was told by court order to bring the guidelines for the proper use of information to the notice of their staff, but that judgment was disregarded for years. To a considerable extent, this supports the fear that the law is powerless. Flagrant violations of confidence and sentiments such as "they will do what they like, no matter what, and who is to stop them?" are running rampant.

1.4 Fear, Uncertainty & Doubt

The fear of privacy loss as a consequence of large-scale application of technology was further fuelled by books and investigations covering violations of privacy and the ways and means to do so. Particularly *The Naked Society* by Vance Packard (1964) was responsible for the sentiment, followed by two influential publications about Big Data *avant la lettre* by Alan Westin: *Privacy and Freedom* (1967) and *Databanks in a Free Society* (1972).

Eventually, after *Database Nation: The Death of Privacy in the 21st Century* (2001) by Simson Garfinkel, the general public was completely confused. FUD, the familiar *Fear, Uncertainty & Doubt*, had definitively become the standard. At the same time, this was the main point of the criticism. Was it true that nothing at all was being done about this kind of practices? We can quite well understand that people tended to respond to fears and facts from the past just to be on the safe side, but what is the actual truth?


"A graphic and blistering indictment..."
—Ralph Nader
Database Nation
THE DEATH OF PRIVACY IN THE 21st CENTURY
Simson Garfinkel

Four lessons learned from the widespread fear during the early Big Data era

1. Without pressure from the outside, organizations are unlikely to change their behavior. Corrections can be effected through public fear and agitation.
2. The real fear concerns the improper use of data by third parties, especially if this happens deliberately, as in the case of data trade.
3. Eventually, indignation about the practices of American credit-rating companies resulted in the 1973 *Code of Fair Information Practices*, followed by the *Swedish Data Act*. Both are based on five principles of proper management of personal information, i.e.:
   - There must be no secret data collection.
   - People should be able to check what has been collected about them and how that is being used.
   - Use of data for other purposes is only allowed after the person in question has given his/her permission.
   - A person should be able to correct or amend his/her Personally Identifiable Information (PII).
   - Every organization creating, managing, using or disseminating PII, has to guarantee the reliability of those data for the intended purpose and make sure the information cannot be misused.
4. Another lesson to be learned from early Big Data history is that valuable time passes between the introduction of rules and regulations and the actions based on such rules and regulations. Therefore it is reasonable for people to be anxious about some parties having an opportunity to ignore the law for a longer time before mending their ways.

1.5 Privacy by Design as solution track

Anyone would think that institutes are focusing less on personal security and privacy than on the business opportunities and efficiency gains offered by new technology. Personal security is not naturally embedded in the system at the outset – it follows at a later stage. It took quite a while, for example, for credit card companies to start texting a verification message after a transfer.

In *Unsafe at Any Speed* (1965) the activist Ralph Nader, who also wrote the foreword to *Database Nation* (2001), analyzed the lack of interest with regard to personal security on the part of the automobile industry. The subtitle of the book is *The Designed-in Dangers of the American Automobile*, but dangers and negative effects need to be neutralized all along the line by building in countermeasures, Nader says:

Join the conversation

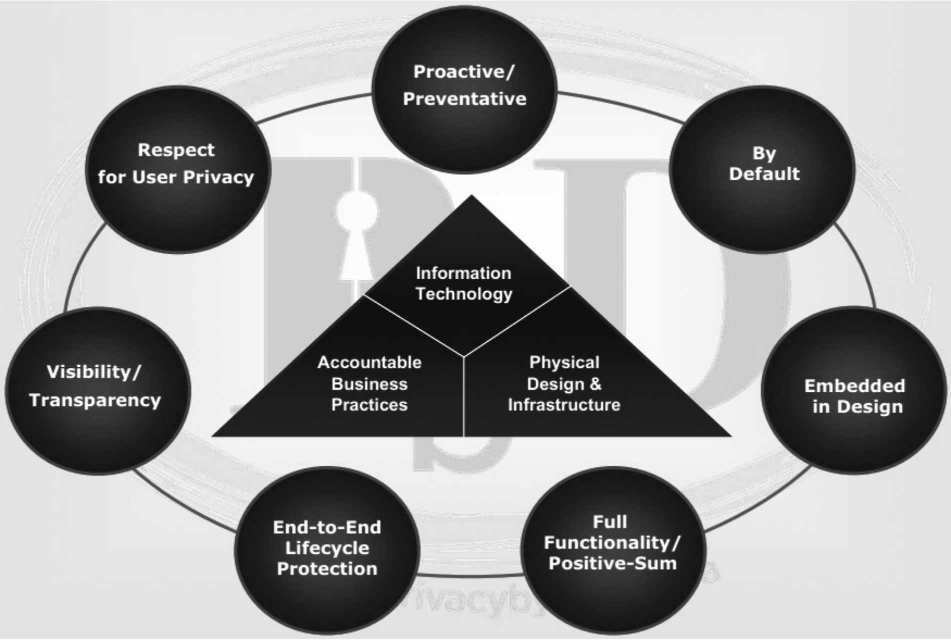
PbD question 2
Is personal information in your IT systems secure by definition, so that no one needs to worry about this?

http://bit.ly/vintR3Q2

> *A great problem of contemporary life is how to control the power of economic interests which ignore the harmful effects of their applied science and technology.*

Safety for the driver, passengers and the environment – it is all part now of the design and therefore of the business. One might say that Privacy by Design, also called the Golden Standard, is the safety belt, the cage, the airbag and the particulate filter of the Big Data business. Nowadays these things are built in at the outset. Privacy by Design is the ideal way forward when it comes to the simultaneous designing and adaptation of technology, procedures and regulations, with a view to assuring optimal safety and guarantees. The harmful effects and risks of driving a car have not been entirely removed, but certainly diminished to a great degree.

Likewise, the interest of stakeholders in the "safety" of personal data will continue to grow. Security and control should be an integral part of the design of systems as well as the eco-system within which they are functioning. This is conducive to the win-situation for all parties and the flourishing of economic models and opportunities, as was earlier explained by the Clinton administration in its *Framework for Global Electronic Commerce.*


Proactive/ Preventative
Respect for User Privacy
By Default
Information Technology
Accountable Business Practices
Physical Design & Infrastructure
Visibility/ Transparency
Embedded in Design
End-to-End Lifecycle Protection
Full Functionality/ Positive-Sum

PbD
www.privacybydesign.ca

As privacy, data protection and personal information represent such high economic and relational value, Ann Cavoukian, the Canadian Information and Privacy Commissioner and "mother" of Privacy by Design, proposed these seven basic principles around the core of each organization, i.e., technology, design and infrastructure, and the operation itself:

1. Privacy by Design means that you take proactive and preventive action: not reactive – no repairs afterwards.
2. Privacy guarantee needs to be the default setting.
3. Privacy needs to be embedded in the design.
4. Go for full functionality: not a poor trade-off but a clearly positive balance.
5. Solutions need to be totally conclusive and unequivocal: end-to-end security at all times.
6. Ensure full visibility and transparency: openness is your leitmotiv.
7. Deal with privacy respectfully: particularly by focusing attention on the individual.

These principles are further operationalized in the conclusion of this report and you are reminded of them by the Privacy by Design (PbD) questions in the margin.

1.6 Our landscape of technology and privacy in a nutshell

The book *Technology and Privacy: The New Landscape*, which was published over fifteen years ago, contains an apt definition of digital privacy. The ensuing fear and hope are also touched upon, and the concept of Privacy by Design is also put forward from converging perspectives, albeit before the term truly existed:

> *Privacy is the capacity to negotiate social relationships by controlling access to personal information. As laws, policies, and technological design increasingly structure people's relationships with social institutions, individual privacy faces new threats and new opportunities. [...]*
>
> *The essays in this book provide a new conceptual framework for the analysis and debate of privacy policy and for the design and development of information systems. The authors are international experts in the technical, economic, and political aspects of privacy; the book's strength is its synthesis of the three.*

Here we give a brief explanation of a number of central concepts (we also refer to "Literature and illustrations" at the end of this report).

Privacy-Enhancing Technologies

Technology and Privacy: The New Landscape *contains a chapter by Herbert Burkert entitled "Privacy-Enhancing Technologies (PETs): Typology, Vision, Critique." This emeritus professor is currently in charge of the research center for Information Law at the University of Sankt Gallen, Switzerland.*

Privacy-Invasive Technologies

One year later, in 1998, the Australian e-business consultant Roger Clarke placed the abbreviation PITs – Privacy-Invasive Technologies – opposite PETs. An up-to-date overview can be found on the PET wiki of the Center for Internet and Society.

Dataveillance

The Dataveillance & Information Privacy *pages of Roger Clarke provide an interesting overview of PITs, PETs and their context. The term* dataveillance *was coined by Clarke. He discussed the concept in the article "Information Technology and Dataveillance" in the* Communications of the ACM *magazine of May 1988. In addition to* surveillance *and* dataveillance *you may nowadays also come across the terms* sousveillance *and* uberveillance.

PETs and Privacy by Design

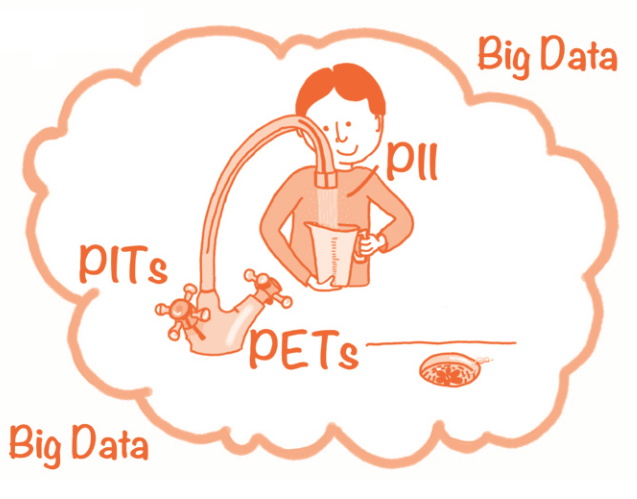
Recent literature on PETs and Privacy by Design:

- *the* Handbook of Privacy and Privacy-Enhancing Technologies *(2003), devoted to intelligent software agents;*
- Privacy-Enhancing Technologies: A Review *by HP Laboratories (2011);*
- Privacy by Design in the Age of Big Data *by the Canadian Information and Privacy Commissioner Ann Cavoukian and IBM's Big Data guru Jeff Jonas (June 2012);*
- *the report* Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices *by Ann Cavoukian (December 2012).*

Privacy by Design and PETs are in a process of rapid development

The relation between Personally Identifiable Information (PII), PITS, PETS and Privacy by Design is very much in the making. A critical view is provided by the article "Regulating Privacy By Design" (2011) written by Ira Rubinstein, a Senior Fellow in the Information Law Institute of the Center for Democracy and Technology, among other things. Rubinstein has doubts about the worldwide enthusiasm with which Privacy by Design and PETS have been greeted in recent years. The thing is that new worlds are hidden behind these concepts and this is where the work really begins, amidst rapidly developing technologies and data flows.

During the last few decades, a lack of clarity about and mistakes in the collection, storage, use and dissemination of personal information have given digital technologies – which enabled all this in the first place – a reputation of Privacy-Invasive Technologies (PITS). To prevent us from having to undergo a ruthless cold shower, we installed a faucet of rules, so to speak. In this way the privacy invasions of cold PITS could be dosed and, by adding hot water in the form of PETS, the water is now no longer ice cold but pleasantly warm. The regulated dataflow that we collect in a measuring jug stands for our Personally Identifiable Information (PII). If too much of it is tapped off, or if it turns out to be a cold shower after all, then down the drain it will have to go – which leaves us with the choice of whether or not to try again. The PII water serves to irrigate the economic relationship with all kinds of service providers.



René Speelman, 2013

It is a striking analogy and indeed: PII, PITS, PETS and the companion Privacy by Design collectively form the basis to doctor privacy security, the aim being to prevent privacy invasions with the help of advanced digital technology.

PETS and Privacy by Design are a major supplement to the original "well" of Fair Information Practice Principles (FIPS), which have no explicit affinity with technology. The development of the technology-oriented Privacy by Design, and consequently, the PETS combined with transparency about and options within business practices and information systems, is a necessary Total (Personal) Data Management approach. All conceivable stakeholders in and outside organizations need to be actively involved and take their *Don't Be Evil* responsibility.

This is why Ann Cavoukian, among others – the "mother" of Privacy by Design – keeps going on about openness and transparency. The goal is "PII for everyone" in a sound economic context. Of course, smart technological PET solutions such as Differential Privacy should be an integral part of this. However, as in the case of PITS, the unbridled dataflows of smart energy meters, for example, and of consumption meters and biometric systems may cause anxiety. The ensuing effects can only be judged by experts, so clearly more technological expertise is required.

With advancing digital technology, optimal privacy and confidence will remain a mathematical limit. However, the situation remains the same and so we have to proceed with concrete and critical action and with the help of a comprehensive approach. In this context, the report by the American Federal Trade Commission *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012) mentions the technology-oriented Privacy by Design as the first matter of importance, combined with simple options for consumers, and transparency. The traditional privacy approach remains important, but a comprehensive technological focus now has the highest priority.

2 What is privacy?

2.1 A first outline 21
2.2 Privacy is a fundamental human right 22
2.3 Privacy comes in different flavors 22
2.4 Privacy is a matter of human civilization 24
2.5 Privacy is essential to the economy 24
2.6 Privacy is personal Total Data Management 25
2.7 Privacy is a matter of trade-offs 27
2.8 Privacy is fear, uncertainty and doubt 29
2.9 Privacy and Big Data 32
2.10 A game to practice privacy 35

2.1 A first outline

Assuming that privacy is a fundamental human right, that there are different flavors, that privacy is a matter of human civilization, as some say, and essential to the economy, is it not a downright shame that there is so much fear, uncertainty and doubt at the moment?

This is all the more true for digital privacy and the value of Personally Identifiable Information: in commercial transactions, in health care, for energy management, in the relationship between citizens and authority etc. Making personal and behavioral data available in exchange for efficient tailor-made service provision can engender an excellent deal with institutions, companies and authorities, as long as we know what is happening to our data and what the risks are. If this is known and arranged with a view to the future, we can then make deliberations and agreements and, as it were, take our Vendor Relationship Management (VRM) into our own hands or tender it out.

To some extent, fear, uncertainty and doubt are just part of our nature, as privacy is typical of the fragile individual who has to stand his ground in the vortex of modern society with all the conflicts of interest that are part and parcel of it. In this digital era of more and more Privacy-Invasive Technologies and data surveillance, no efforts must be spared to remove the sting of fear.

This is done by focusing on personal Total Data Management – in other words, control over our PII, our Personally Identifiable Information. In this context, technology is central in the balance – or race, if you like – between Privacy-Invasive Technologies (PITs) and Privacy-Enhancing Technologies (PETs).

Ideally, this balance has to be established in practice through Privacy by Design in a “fully automatic” and extremely meticulous manner. It means that the PETs have to be

Join the conversation

PbD question 3
Are privacy requirements an integral part of the design and architecture of your IT systems and business practices?

http://bit.ly/vintR3Q3

integrally adjusted and geared to the correct procedures, regulations, physical environment etc., as proposed at the end of section 1.5 and in the conclusion.

For your reference, in this chapter we define the (digital) privacy theme by means of seven different denominators. We conclude with the increasingly important role of Big Data and a game to practice privacy in social networks.

2.2 Privacy is a fundamental human right

> *No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation.*
>
> Universal Declaration of Human Rights, 1948, section 12

In the Universal Declaration of Human Rights of the United Nations, privacy is an unalienable human right and is mentioned as such in charters, constitutions, regular laws and treaties throughout the world. Resolution A/HRC/20/L.13 of July 2012 of the United Nations Human Rights Committee – about “promoting, protecting and having human rights on the Internet” states that all human rights need to be protected offline and online, particularly freedom of speech. Moreover, this is conducive and even vital to economic transactions.

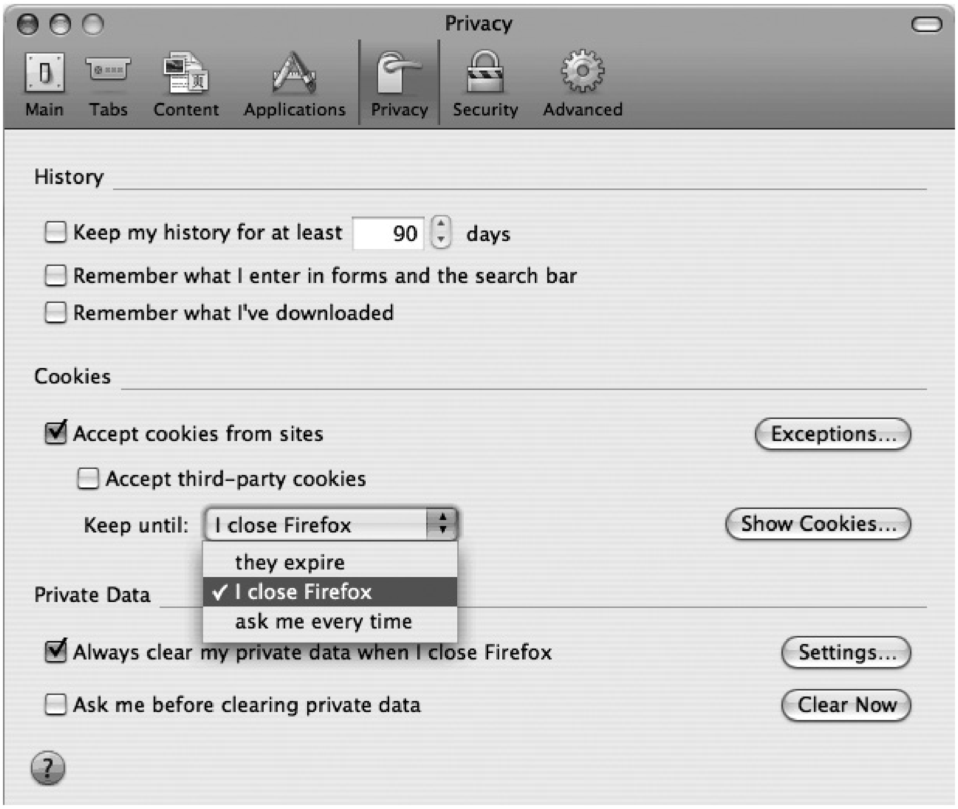
2.3 Privacy comes in different flavors

The first privacy act dates from 1361, when peeping and eavesdropping were made punishable in England. Modern views with regard to privacy distinguish different categories – such as personal, informational, organizational, spiritual and intellectual – of “bodily privacy (private parts), territorial privacy (private places), communications privacy (private messages), information privacy.” Our online privacy is usually called *ePrivacy*. Digital privacy is not necessarily online and, according to the letter, informational privacy need not necessarily be digital. The diagram on page 26 gives an indication of what the term “digital Personally Identifiable Information” nowadays means.

Apart from the fact that there are different kinds of privacy, the level of privacy may also differ. An example of this can be seen in our browser settings:

Privacy
& Free
Speech
It's Good
for Business

http://www.dotrights.org/business/primer



History

☐ Keep my history for at least 90 days

☐ Remember what I enter in forms and the search bar

☐ Remember what I've downloaded

Cookies

☑ Accept cookies from sites

☐ Accept third-party cookies

Keep until: I close Firefox

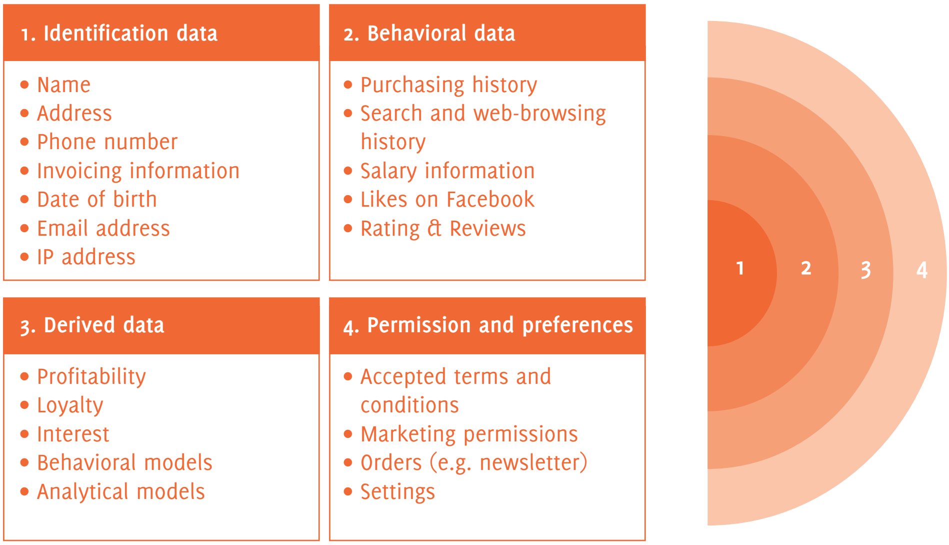
- they expire
- ✓ I close Firefox
- ask me every time

Private Data

☑ Always clear my private data when I close Firefox

☐ Ask me before clearing private data

Levels of privacy are also found in the consumer data collected by organizations (illustration by Magenta Advisory):



1. Identification data

- Name
- Address
- Phone number
- Invoicing information
- Date of birth
- Email address
- IP address

2. Behavioral data

- Purchasing history
- Search and web-browsing history
- Salary information
- Likes on Facebook
- Rating & Reviews

3. Derived data

- Profitability
- Loyalty
- Interest
- Behavioral models
- Analytical models

4. Permission and preferences

- Accepted terms and conditions
- Marketing permissions
- Orders (e.g. newsletter)
- Settings

It is the uncontrolled combination of this kind of digital data that is currently a source of great concern in terms of privacy.

2.4 Privacy is a matter of human civilization

The well-known and even somewhat controversial Russian-American writer Ayn Rand (1905-1982) equated our social civilization concisely with optimal privacy:

> *Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men.*
>
> A. Rand (1943), *The Fountainhead*

In the eighteenth century, the French political thinker Jean-Jacques Rousseau rather ironically put it as follows:

> *The first man who, having enclosed a piece of ground, bethought himself of saying "This is mine," and found people simple enough to believe him, was the real founder of civil society.*
>
> Rousseau (1754), *Discourse on the Origin and Basis of Inequality among Men*

We need not necessarily agree with the nuances of these observations to appreciate that, from a digital and online point of view, the difference between mine and thine is becoming increasingly obscure nowadays, as is the distinction between public, personal and secret, or that between free of charge and paid for. What does that say of our "civilization"? Are we losing it; did not social civilization always have an adverse effect; should we move with our times and stop moaning about how human constructs such as privacy are shifting the way they do?

2.5 Privacy is essential to the economy

The article "Privacy: Its Origin, Function, and Future" (1979) in which the American economist and professor Jack Hirschleifer emphasizes the economic dimension of privacy, starts with Rousseau's view. The economic dimension explicitly manifests itself in the influential *Framework for Global Electronic Commerce* (1997) by the Clinton administration, as we have seen in section 1.2.

Privacy, Hirschleifer said in 1979, is nowadays not so much a traditional matter of "secrecy" – of withdrawal and of keeping things under cover. It is rather the "autonomy within society" that is central. This autonomy of individuals and groups is synonymous with active economic action. The way in which this could be related to uncertainty and information was something Hirschleifer was specialized in: what does it mean when people do not really know and cannot assess what is known about them? Privacy was “a way of organizing society” rather than of “withdrawal,” as Hirschleifer literally underlined it in his article.

2.6 Privacy is personal Total Data Management

According to the writer Gabriel García Márquez, each individual has three kinds of lives: a public life, a private life and a secret life. As early as 1948, George Orwell described in his book *1984* what devices and the Internet could do in this context:

> *It was terribly dangerous to let your thoughts wander when you were in any public place or within range of a telescreen. The smallest thing could give you away.*

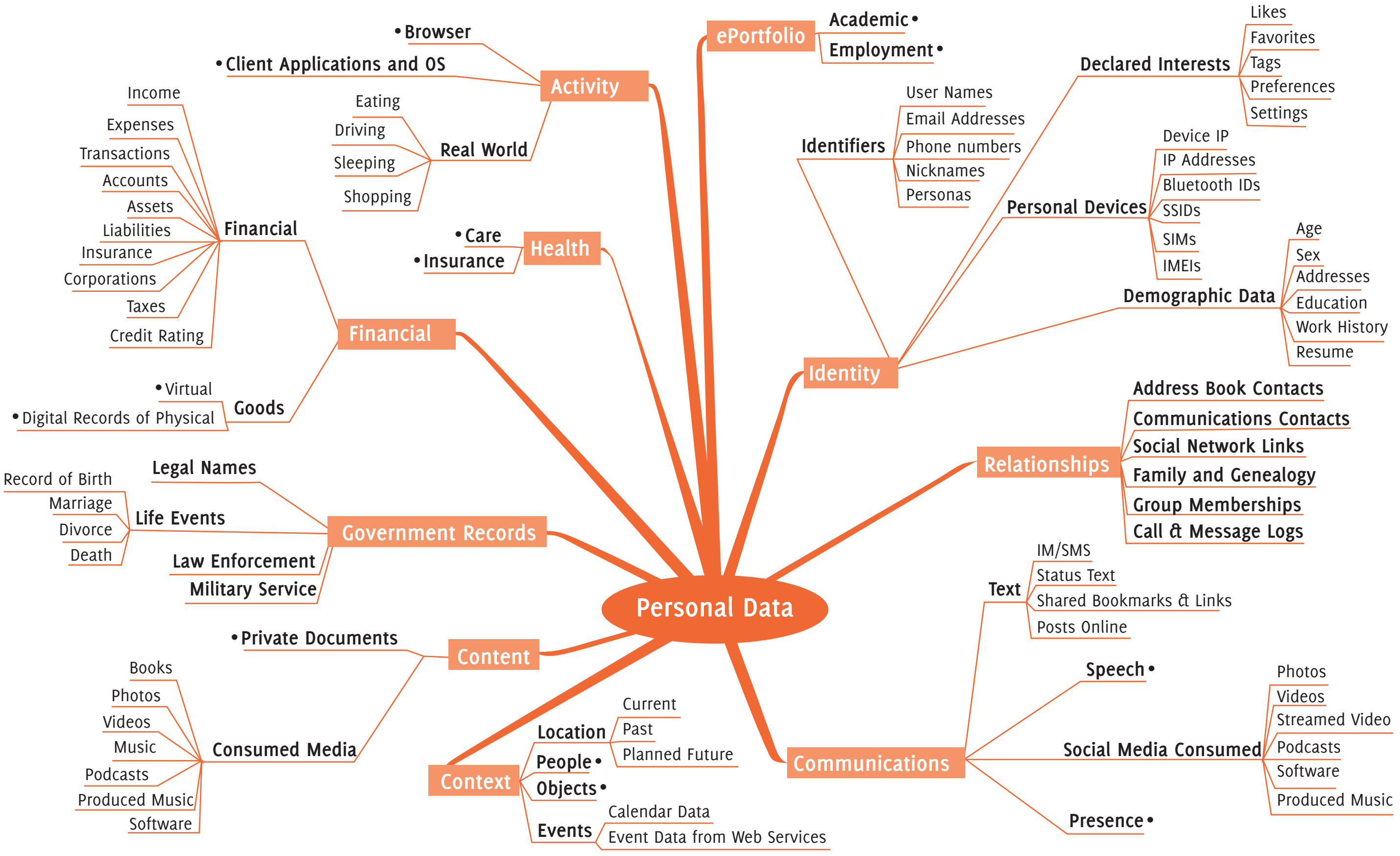
In those days that was a gross exaggeration and it still is in our time, fortunately, but it certainly reflects the fear with which we experience the present *surveillance & dataveillance society*. In the street and online, all conceivable dataflows can be monitored on a permanent basis.

It seems that the only place where we have some privacy is in the toilet at home. It is not without reason that *privy* is related to *privacy* and *private*. The title of this *Digital Life eGuide* plays with that relationship in meaning:

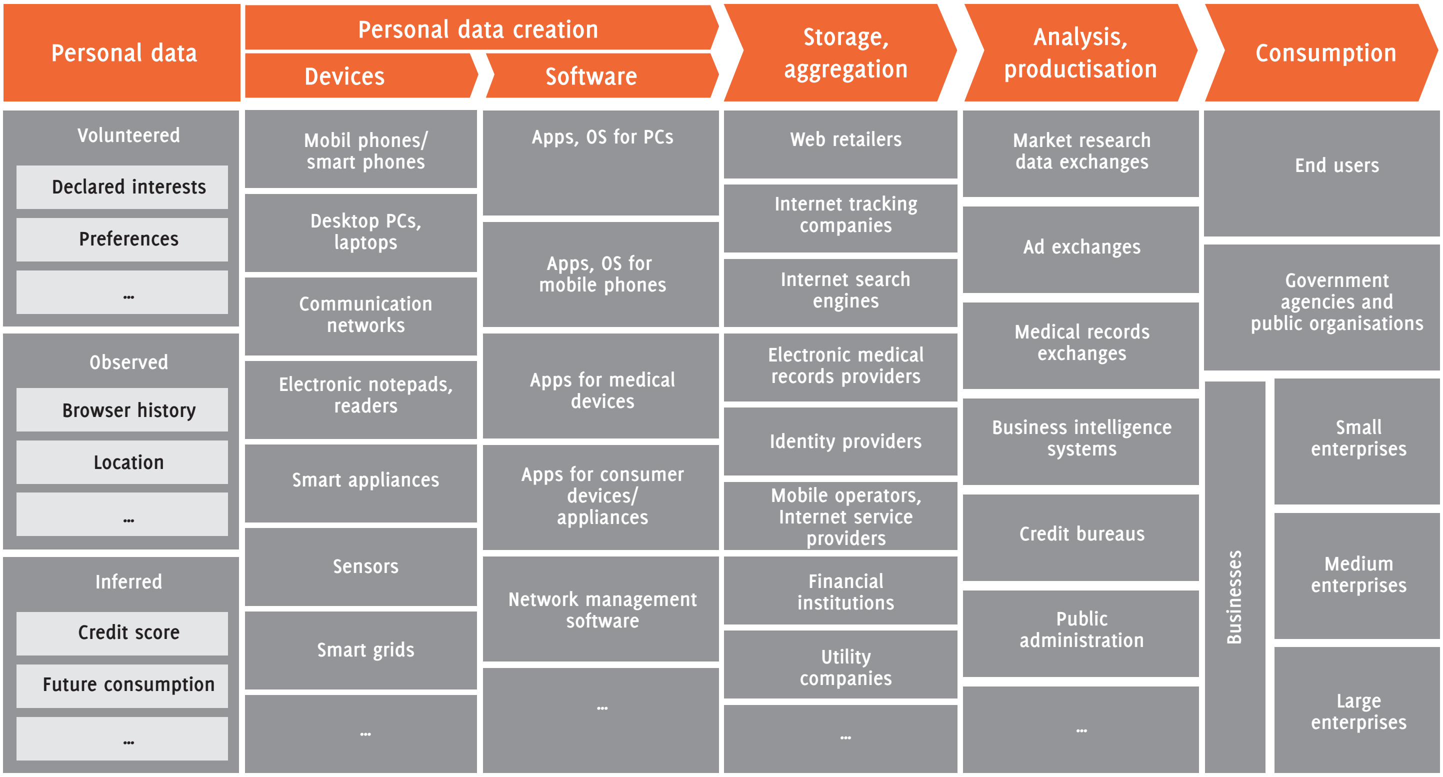
The difference between public, private and secret is the essence of the privacy theme, not in the least in the context of private data and other personal information. Their protection – data protection, *Datenschutz* – is covered by law.

The current European *Data Protection Directive* will be changed into a binding law for all member-states, and is meant to become effective as of 2015. With all the digital activity that we have today, the distinction between public, private and secret is more fluid and fuzzier than ever.

Kaliya Hamlin, also known online as Identity Woman, made the mindmap below showing the cloud with personal digital data or Personally Identifiable Information (PII) that is hanging around us all to a greater or lesser extent: partly public, partly private and partly secret. All in all, this provides a complete picture at any time of who we are, what we think, and what we find interesting; in other words, what we might be ready to pay for or what we might be blackmailed with one way or another.



In diagram form, according to the World Economic Forum report *Personal Data: The Emergence of a New Asset Class*, the PII life cycle from creation to consumption looks as follows:



Personal data

- Volunteered
  - Declared interests
  - Preferences
  - ...
- Observed
  - Browser history
  - Location
  - ...
- Inferred
  - Credit score
  - Future consumption
  - ...

Personal data creation

Devices

- Mobil phones/ smart phones
- Desktop PCs, laptops
- Communication networks
- Electronic notepads, readers
- Smart appliances
- Sensors
- Smart grids
- ...

Software

- Apps, OS for PCs
- Apps, OS for mobile phones
- Apps for medical devices
- Apps for consumer devices/ appliances
- Network management software
- ...

Storage, aggregation

- Web retailers
- Internet tracking companies
- Internet search engines
- Electronic medical records providers
- Identity providers
- Mobile operators, Internet service providers
- Financial institutions
- Utility companies
- ...

Analysis, productisation

- Market research data exchanges
- Ad exchanges
- Medical records exchanges
- Business intelligence systems
- Credit bureaus
- Public administration
- ...

Consumption

- End users
- Government agencies and public organisations
- Businesses
  - Small enterprises
  - Medium enterprises
  - Large enterprises

Personal digital data in all shapes and sizes collectively form the domain of digital privacy. What matters then is not that our valuable PII remains secret at all costs, but rather that we can control which information we are prepared or are not prepared to exchange or sell, as Jack Hirschleifer suggested with his *autonomy* in 1979. To ensure an optimal enforcement of that autonomy as an organizing and economic principle, we need to be constantly aware of the way our PII relates specifically to the two overviews above, of what "leaks away" unintentionally, and of how that information is used.

2.7 Privacy is a matter of trade-offs

When we say that privacy – or simply feeling free or good – is essential to a well-oiled digital economy, the economic concept of *trade-off* immediately comes to mind. Situation-wise and individually we make different choices as to what we will or will not be prepared to allow when it comes to collecting, sharing and using information. After all:

- *Privacy is "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."*

- *There is no free lunch: We cannot escape the trade-off between locking down information and the many benefits for consumers of the free flow of information.*

Berin Szoka, Senior Fellow, The Progress & Freedom Foundation,
7 December 2009

Privacy is an object of exchange on many fronts: *trade-off is the name of the game*. When parents are nosing in their children's Facebook posts, there is a trade-off between privacy and upbringing. In our digital age, we are even referring to the *privacy paradox:* the wish, on the one hand, to remain anonymous, and the practically unbridled urge to share one's deepest feelings with the world on the other.

Another well-known example is the trade-off between privacy and health. An Electronic Health Record may encroach on our privacy, but we benefit from it in terms of expectancy and quality of life. The same is true of the most current cookie analyses on the Internet and a better service by organizations to customers and prospects. There are various kinds of privacy trade-offs, for instance:

- privacy versus upbringing
- privacy versus health
- privacy versus the fight against fraud
- privacy versus better service
- privacy versus efficient energy systems
- privacy versus self-expression
- privacy versus security.

As (digital) privacy is a trade-off, it is by definition an economic commodity. Faithful to the upright tradition of Hirschleifer, this is also argued by Alessandro Acquisti, co-director of the Carnegie Mellon Center for Behavioral Decision Research, in the paper *The Economics of Privacy*. The economy that is increasingly developing around privacy goes from *mining* and selling personal information to the purchase of products aiming to protect our privacy as consumers.

One of the main trade-offs is privacy versus security, in the sense of being able to move in the physical and digital space without seeing one's physical and ethical integrity challenged. We find it acceptable when the government checks the Internet searching for child porn, we agree to camera surveillance and having our fingerprints taken, etc. But at the same time, skepticism and fear are growing. Nowadays, the Big Brother sentiment is at odds with the opportunities offered by Big Data, in both a commercial and a social sense.

Long before data volume, variety and velocity were topics, Big Brother was already an issue. The history of the records, the censuses, all sorts of recordings and later the population statistics are closely connected with this skepticism, which is often government-oriented. In addition, digital and media go hand in hand nowadays, which has its most appreciable effect for the average citizen in the means used by our surveillance society. For example, this theme was extensively elucidated in *A Report on the Surveillance Society for the [British] Information Commissioner* (2006) by the Surveillance Studies Network.

Lively debates are going on about the trade-off of security versus privacy and the necessity of a trade-off is even contested by people such as Daniel Solove, for example, in his book entitled *Nothing to Hide: The False Trade-off between Privacy and Security* (2011). The argument of the VRM camp is that, thanks to Vendor Relationship Management, privacy need not be a trade-off at all.

In the American Civil War of 1861-1865, Big Brother sentiment received a powerful boost when the population register was used to locate possible military camps in the Southern states. The rise of totalitarian regimes and ideologies, and their disastrous effects, inspired science fiction authors to create scenarios that are so dystopic that they dispel all inclination for any Big Data-like society whatsoever. We are familiar with the classics of the genre:

◆ **1924**	*We*, Yevgeny Zamyatin
◆ **1932**	*Brave New World*, Aldous Huxley
◆ **1948**	*1984*, George Orwell
◆ **1951**	*Foundations*, Isaac Asimov
◆ **1951**	*Fahrenheit 451*, Ray Bradbury

Each of these books lets us have a specific look at how the individual's behavior can be watched and monitored with the help of technology. Later, at the time of the Cold War, America had far more confidence in the government and people were more afraid of the enemy than of the Big Brother in their own country who was spying on them. Senator McCarthy's hunt for communists in the fifties, for example, had a broad support basis among the population.

Join the conversation

PbD question 4
How do you deal with privacy versus security? Do you think they can exist in perfect harmony?

http://bit.ly/vintR3Q4

2.8 Privacy is fear, uncertainty and doubt

As early as 1966, William Douglas, the longest serving member of the Supreme Court of the United States, said the following about uncertainty with regard to technology-related privacy:

> *We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government.*

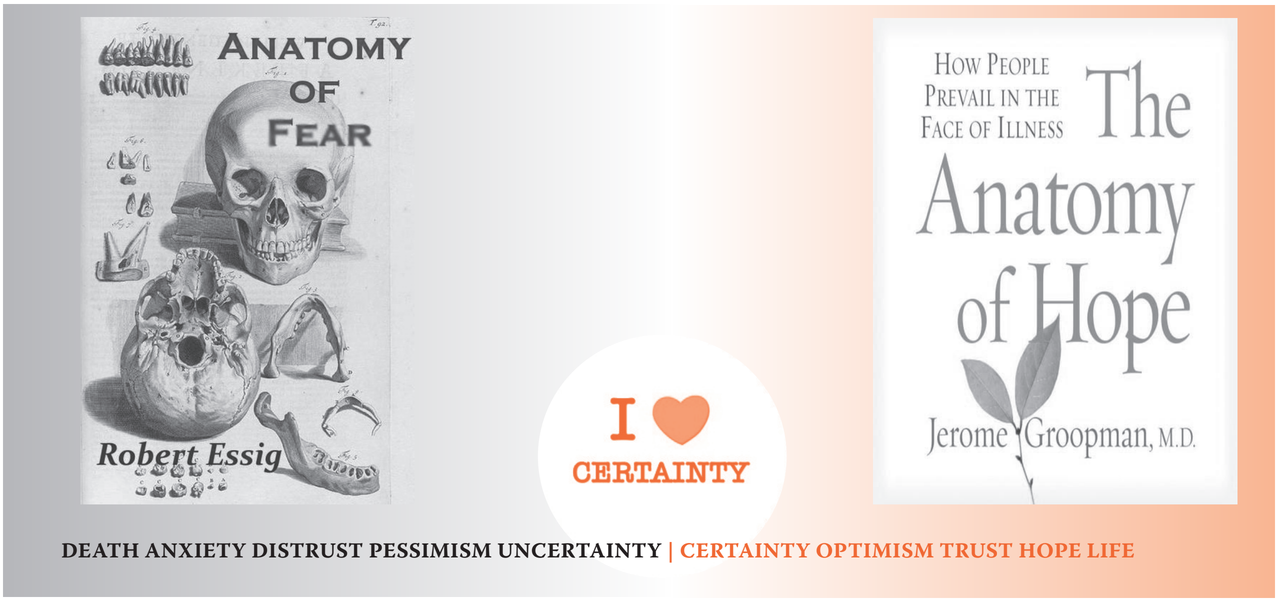
Nowadays living in a surveillance and dataveillance society is considered acceptable. On the one hand, we have to cope with PITS (Privacy-Invasive Technologies) and, on the other, with PETS (Privacy-Enhancing Technologies). The American National

Security Agency is currently building a quantum supercomputer, named Vesuvius, to enable constant monitoring of digital data flows of literally everything and everyone in the world. In the name of national security and protection of the democracy, and in all secrecy of course.

Google™
Web Images Groups News Froogle Local more »
Google Search
I'm Feeling Lucky
FEDS

Bob Englehart in the Hartford Courant*, 22 January 2006, http://www.gsmnation.com/blog/2012/09/25/the-fbi-wants-permission-to-wire-tap-your-facebook-account/google-and-the-feds/*

This secrecy also covers the use of Palantir investigation technology, for example, and the NSA's relationship with Google, among others. This extends far beyond *Database Nation: The Death of Privacy in the 21st Century* by Simson Garfinkel (2001). The spectrum of *Fear, Uncertainty & Doubt*, covering fragile individuals and minority groups, can be represented as follows:


ANATOMY OF FEAR
Robert Essig
I ♥ CERTAINTY
How People Prevail in the Face of Illness
The Anatomy of Hope
Jerome Groopman, M.D.
DEATH ANXIETY DISTRUST PESSIMISM UNCERTAINTY | CERTAINTY OPTIMISM TRUST HOPE LIFE

We see five categories to the left and five to the right of the thin blue line that marks our fragile sense of privacy. Directly linked to the central yearning for security, which is closely connected with the familiar trio of *data – information – knowledge/understanding*, is the methodical doubt expressed by Descartes in the seventeenth century. This *doubt* may all too easily turn into fear if we fail to dispel it. As fear has a paralyzing effect, we wish to deal with it adequately by trying to analyze it, to explain its components, to define its anatomy, so that we can neutralize it.

In this context, it is remarkable that an anatomy of hope, the opposite of fear, is also often described from a negative perception; in the illustration above, it is from the standpoint of illness. And indeed, we often regard our privacy as ill, or at any rate we feel that it is developing in an unhealthy direction.

As far as our sense of privacy is concerned, we have extremely negative feelings most of the time, being afraid of Big and Little Brothers who are threatening and overshadowing us, particularly from a technological point of view. It has been repeatedly stated of late that the best thing to do is forget all about privacy as a privilege in this digital age.

It is this very aspect of "forgetting" that has become a big issue thanks to the Internet, all databases in existence, and also Big Data. *The Right to Be Left Alone* has been further refined into *The Right to Be Forgotten* (2012) by EU commissioner Viviane Reding. But one may well wonder if this can be guaranteed and, if so, through which technologies and procedures. With Abine's DeleteMe app? There is an enormous danger that we will eventually end up in the red zone, with all the economic and social consequences. In this way, privacy may well turn into a showstopper for the wonderful opportunities that datamining and Big Data have to offer in many fields of interpersonal relations.

The Chaos Computer Club raises the alarm

In this context, managing Big Data clumsily is one side of the matter, while deliberately breaking rules is another. These extremes can be illustrated with two examples from Germany. At the annual conference of the Chaos Computer Club in late 2011, it became clear that the smart energy meters of the supplier, Discovergy, were poorly secured. Energy consumption was measured every two seconds for no apparent reason and, in addition, the dataflows were not encrypted. In every household, the consumption per separate device could thus be accurately recorded, with all the consequential possibilities for an analysis of viewing habits and Internet use, for example. The data obtained by the researchers came from "smart meters" that were sealed by way of standard procedure. The poor security might also have enabled hackers – had they managed to penetrate further into the system – to bring the energy supply of millions of households to a standstill.

Without a doubt, the Vesuvius comprehensive data-monitoring project of the above-mentioned secret American National Security Agency puts the matter of digital privacy in a particular light. This is also true of the discovery by the same Chaos Computer Club of a computer virus launched by the German government, also in 2011. The code was capable of completely infiltrating a computer, monitoring all actions, storing them and introducing new viruses. Camera, screenshots, Internet telephone traffic, key strokes and of course all hard disk files were completely under control of the monitoring software, reported the *Frankfurter Allgemeine Zeitung*.

2.9 Privacy and Big Data

Ever since the development of media technology such as photography, telephony and telegraphy in the nineteenth century, privacy has become an increasingly important point of interest. The maxim *Privacy Is the Right to Be Left Alone* originated in the America of the 1890s. This is when the development of technology and our need of privacy were seriously at odds for the first time:

> *Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be left alone." [...] Numerous [...] devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the rooftops."*

To date, the validity of this quotation still stands. Without the photography, the newspapers and the word "mechanical," which we have deliberately omitted from the quotation, no one could have suspected that these words date from 1890, and have been taken from the article "The Right to Privacy" by Samuel Warren and Louis Brandeis in the *Harvard Law Review*. In fact, this is what primed the entire modern debate on privacy. And even today, photography and paparazzi occupy center stage when it comes to privacy issues.

That Big Data is an extra cause of concern these days also became evident when Schufa, the largest German credit-rating firm, announced that it intended to link information from Twitter, Facebook and LinkedIn to its 66-million customer database for the sake of better profiles.

This attack on the people's right to have control over their own data gave Germany reason to fear "American circumstances." Ilse Aigner, the Minister with consumer rights in her portfolio, stated that social networks must not be systematically used to assess credit applications.

In 2012, the following three articles, dealing with the combined theme of privacy, data protection and the rise of Big Data, were among those that caught the eye:

- The first one was entitled "Privacy in the Age of Big Data: A Time for Big Decisions," and was published in the February issue of *Stanford Law Review*.
- Number two, "The Challenge of Big Data for Data Protection," first saw the light of day in the May issue of the *Oxford Journal on International Data Privacy Law*.
- And the third, "Privacy by Design in the Age of Big Data," came from the Office of Ann Cavoukian, the Information and Privacy Commissioner of Ontario, in June. Her co-author is IBM's Big Data guru Jeff Jonas.

The article "Big Data for All: Privacy and User Control in the Age of Analytics" on the website of the *Stanford Law Review* magazine (February 2012) gave a good idea of what is going on with privacy and data protection in the light of Big Data. The reasoning is as follows: Big Data is reality; it is extremely valuable, but at the same time it fuels uneasiness about privacy. So a good balance needs to be created between organizations and individuals. At the very beginning of the book, authors Omer Tene and Jules Polonetsky make the following seven points:

The Big Data reality

1. *The amount of information at the disposal of organizations and authorities has expanded, due to developments in data mining and analytics, and the enormous increase in computing power and data storage.*
2. *Raw data can now be analyzed without the help of structured databases. This way, it is much easier to demonstrate interrelationships, while new unthought-of applications for existing information are beginning to emerge.*
3. *At the same time, the growing numbers of people, devices and sensors that are linked by means of digital networks have caused a revolution in creating, communicating, sharing and accessing data.*

The value and privacy challenge of Big Data

4. *Data are of great value to the world economy as the raw material for innovation, productivity, efficiency and growth. At the same time, the flood of data poses privacy issues that may result in regulations that bring the data economy and innovations to a standstill.*
5. *To find a balance, policy makers need to address a number of the most fundamental privacy concepts, such as the definition of Personally Identifiable Information (PII), the way it can be controlled by the individual, and the principles of minimal and effective use of data.*

A good balance for organizations and individuals

6. *When individuals have data at their disposal in an accessible manner, they can share the wealth of the information. On that basis valuable client applications can be developed.*

7. It is obvious that organizations are obliged to be quite explicit when it comes to their decision criteria, for in a Big Data world it is usually the conclusions that give cause for concern and not the data themselves.

The article "Big Data for All," to be published in the *Northwestern Journal of Technology and Intellectual Property*, provides an overview of the advantages of Big Data in different fields and economic sectors. Subsequently the drawbacks are discussed, and this is followed by a number of central challenges and finally by a number of solutions.

The concept of Privacy by Design provides a fundamental underpinning: the worrisome effect of Privacy Invasive Technologies must be counterbalanced by an intense combination of Privacy Enhancing Technologies, regulations, policy, procedures and responsible behavior by all parties involved.

In this way Big Data, too, should become a win-win situation for all. Politics, businesses, authorities and individuals all over the world are looking forward to seeing that ambition and promise realized.

Privacy, technology and the law

The idea is that in the years to come there will be a huge change for the better in the relationships between privacy protection, digital technology and regulation. This is essential for the development of the economy and of social relationships. In 2011, the 112th American Congress (the Obama I administration) was the first to install a special Senate Committee with the clear name: *Privacy, Technology and the Law*. The committee has the following five main tasks in its portfolio:

- *Supervision of regulation and policy with regard to the collection, use and dissemination of commercial information by the private sector, including behavioral advertising, privacy in social networks and other online privacy issues.*
- *Enforcement and implementation of regulation and policy with regard to the privacy of commercial information.*
- *Use of technology by the private sector to protect privacy, enhance transparency and stimulate innovation.*
- *Privacy standards for the collection, storage and management, use and dissemination of commercial Personally Identifiable Information (PII).*
- *Privacy implications of new or emerging technologies.*

In our Big Data business reality, we are now heading on a worldwide scale toward a fundamental emphasis on transparency and choice, toward “informed consent” and clear “opting out” possibilities for individuals. In this context a balance between PITS and PETS, combined with clear regulations and procedures through Privacy by Design, seems to be the best and most comprehensive solution. This subject is dealt with in Chapter 3.

2.10 A game to practice privacy

Cultivating one’s awareness and individual responsibility is also part of Privacy by Design. For a short time now, a privacy game has been available on http://www.open.edu/openlearn/privacy to practice the new standards and values on social networks. Via “Secret or sharing? Play our Privacy Game” you can decide which information you are willing to share and which you had better keep to yourself. The game offers the opportunity to make a small, valuable and perfectly safe bet with your personal data. Via OpenLearn you are playing the computer alone, but you can also challenge your Facebook friends to a multiplayer version of the privacy game, which still has a closed character.

> *Count not him among your friends who will retail your privacies to the world.*
> Publilius Syrus, ca 50 BC

3 Privacy by Design and the balance between PITs and PETs

(Privacy-Invasive versus Privacy-Enhancing Technologies)

3.1 A new taxonomy of privacy 36
3.2 Personally Identifiable Information and PETS 38
3.3 Privacy according to TNO and TILT 40
3.4 E-privacy-related challenges 42
3.5 Responsible behavior as core value 43

3.1 A new taxonomy of privacy

In January 2006, the *University of Pennsylvania Law Review* published an 84-page article by Daniel Solove, currently a professor at George Washington University Law School. In the article with the same succinct title, to which another 25 experts contributed, Solove presented a new *Taxonomy of Privacy*, linked to technology and information.

Digital innovations have become more and more prevalent, but the abstract legal concept of privacy was and still is insufficiently geared to this situation, to use an understatement. Solove c.s. are hard as nails in their assessment:

> ***Privacy is a concept in disarray. Nobody can articulate what it means.*** *[...] Privacy is far too vague a concept to guide adjudication and lawmaking, as abstract incantations of the importance of "privacy" do not fare well when pitted against more concretely stated countervailing interests. [...] This Article develops a taxonomy to identify privacy problems in a comprehensive and concrete manner.*

The notion of privacy should be fleshed out, not least to ensure its unequivocal character in the context of legislation. By early 2006 we had already made considerable progress in the digital age, but concrete new privacy issues were hardly addressed adequately. It was high time to create a comprehensive and clear regulation that would primarily deal with the activities of individuals, organizations and authorities:

> *Technology is involved in various privacy problems, as it facilitates the gathering, processing, and dissemination of information. Privacy problems, however, are caused not by technology alone, but primarily through activities of people, businesses, and the government. The way to address privacy problems is to regulate these activities.*

From this interesting observation of 2006, we have now – seven years later – come to a point where interest in activities is gradually being combined with the development and enforcement of a good balance: between Privacy-Invasive Technologies (PITs) on the one hand and Privacy-Enhancing Technologies (PETs) on the other. This fundamental and integral approach is known as Privacy by Design. The following taxonomy of privacy by Solove et al., dating from 2006, which displays a clear focus on technology and information, acts as a sounding board in that context:

Information Collection
- Surveillance
- Interrogation

Information Processing
- Aggregation
- Identification
- Insecurity
- Secondary Use
- Exclusion

Information Dissemination
- Breach of Confidentiality
- Disclosure
- Exposure
- Increased Accessibility
- Blackmail
- Appropriation
- Distortion

Invasion
- Intrusion
- Decisional Interference

Join the conversation

PbD question 5
In the context of data protection, do you also believe that it must be possible to destroy information definitively at a given moment?

http://bit.ly/vintR3Q5

3.2 Personally Identifiable Information and PETS

For a variety of reasons and in a variety of ways, organizations have the Personally Identifiable Information (PII) of employees, customers and other parties at their disposal. In this context, the rules for privacy and data protection must be upheld. Well-designed and well-implemented Privacy-Enhancing Technologies (PETS) are the opposite of Privacy-Invasive Technologies (PITS). They aim to realize the required protection in combination with regulations, guidelines, processes, training etc.

Ideally, PETs have a clear connection with what privacy rules require and intend. Therefore the British Information Commissioner's Office describes PET as:

> *any technologies that protect or enhance an individual's privacy, including facilitating access to their rights under the Data Protection Act.*

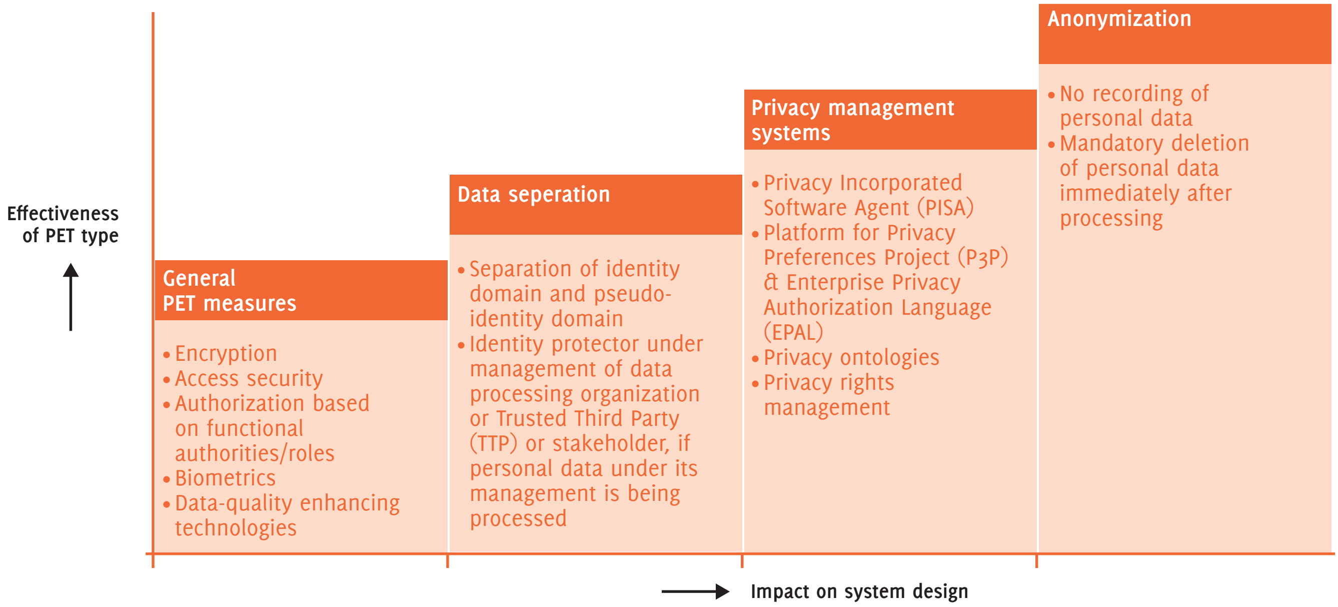
In addition, the European Union emphasizes the role of PETs in the designing of information and communication systems, in such a way that any regulation from the perspective of technology is given a firm basis:

> *The use of PETs can help design information and communication systems and services in a way that minimises the collection and use of personal data and facilitates compliance with data protection rules making breaches more difficult and/or helping to detect them.*

The above-mentioned *Taxonomy of Privacy* by Daniel Solove is a perfectly adequate vehicle for a *Privacy Impact Assessment* framework (see section 4.7) for PETs that intend to prevent privacy-related damage. What is at issue here is what is known as *Fair Information Practices*, the foundation of a digital economy that is worthy of confidence, not least when Big Data are used. Our personal data, our PII or simply our contextual ID come into play here. While thanking Alexander Alvaro, vice-president of the European Parliament, we have reduced the description of his PII pictograms to the following practical set of FIPS *(Fair Information Practice Principles)* on the left.

collect	✓
retain	✓
process	✗
disseminate	✓
sell	✗
encrypt	✗

A concrete overview of PETs is provided by the relevant wiki of the Center for Information and Society: http://cyberlaw.stanford.edu/wiki/index.php/PET. The graph below by Koorn and Ter Hart (2011) provides an overview of the effectiveness of different PET types, compared to the impact on the system design.


Effectiveness of PET type
General PET measures
• Encryption
• Access security
• Authorization based on functional authorities/roles
• Biometrics
• Data-quality enhancing technologies
Data seperation
• Separation of identity domain and pseudo-identity domain
• Identity protector under management of data processing organization or Trusted Third Party (TTP) or stakeholder, if personal data under its management is being processed
Privacy management systems
• Privacy Incorporated Software Agent (PISA)
• Platform for Privacy Preferences Project (P3P) & Enterprise Privacy Authorization Language (EPAL)
• Privacy ontologies
• Privacy rights management
Anonymization
• No recording of personal data
• Mandatory deletion of personal data immediately after processing
Impact on system design

Technology is an indispensable aid, but its success invariably depends on implementation – see Koorn and Ter Hart (2011) for an overview – and adoption. In *Privacy Enhancing Technologies: A Review* (2011), Yun Shen and Siani Pearson of HP Laboratories recommend a focus on the following fields:

- Usability
- Privacy by Design
- Economics of Privacy

As for the last, we usually do not feel that the costs of a considered privacy choice, however small, are worth it nowadays. In practice, the so-called *Willingness to Pay* clearly loses out to the *Willingness to Accept*. A good example is unquestioningly accepting page-long terms and conditions online.

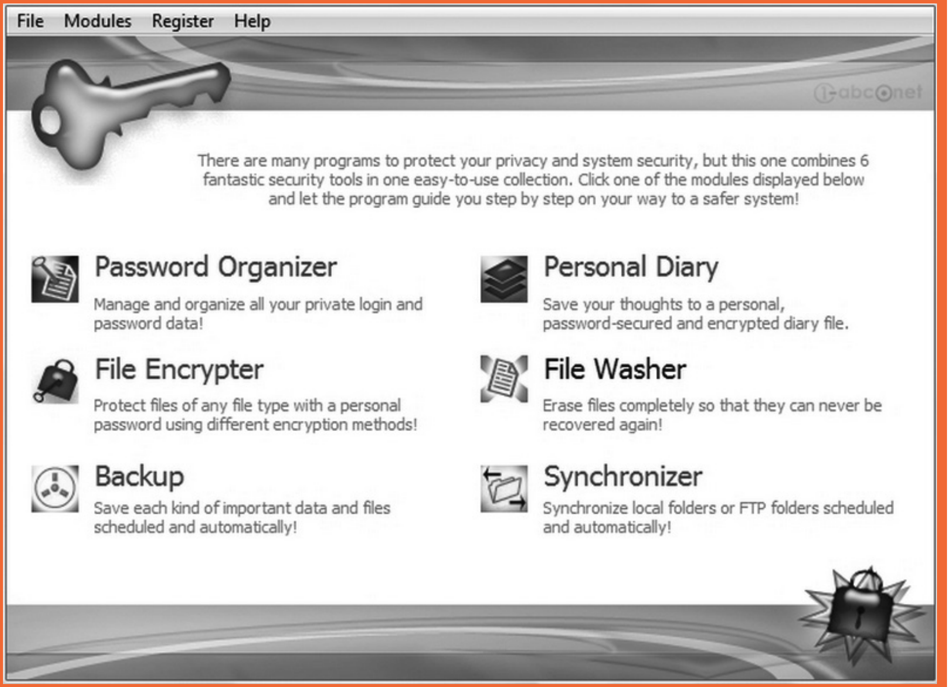
Differential Privacy

In the context of the still extremely relevant theme of database privacy, *Differential Privacy*, which is relatively unknown, needs to be added. It is very difficult to guarantee the individual protection of privacy in databases, even if PII has been minimized. It often turns out that, with a lot of trouble, it is possible to use data from other databases by way of supplement, thus converting the information to the individual level. Differential Privacy neutralizes this re-identification problem by adding white noise, among other things, to the otherwise correct database matter. The quality of the aggregated results is not at stake because of a Differential Privacy approach.

3.3 Privacy according to TNO and TILT

In December 2011, the Dutch organization for Applied Physics Research TNO and the Tilburg Institute for Law, Technology and Society TILT published the report entitled *Trusted Technology: a study into the application conditions for Privacy by Design in the electronic services of the government*. The concept of Privacy by Design is explicitly based on Privacy-Enhancing Technologies (PETS). See, for example, the 350-page *Handbook of Privacy and Privacy-Enhancing Technologies* (2003). That publication is devoted to intelligent software agents.

The PET spectrum has a huge range. This security tool, for aspects such as protected passwords, file encrypter, an encrypted diary file and an option to erase files completely, is a basic PET application at computer level:



There are many programs to protect your privacy and system security, but this one combines 6 fantastic security tools in one easy-to-use collection. Click one of the modules displayed below and let the program guide you step by step on your way to a safer system!

Password Organizer
Manage and organize all your private login and password data!

Personal Diary
Save your thoughts to a personal, password-secured and encrypted diary file.

File Encrypter
Protect files of any file type with a personal password using different encryption methods!

File Washer
Erase files completely so that they can never be recovered again!

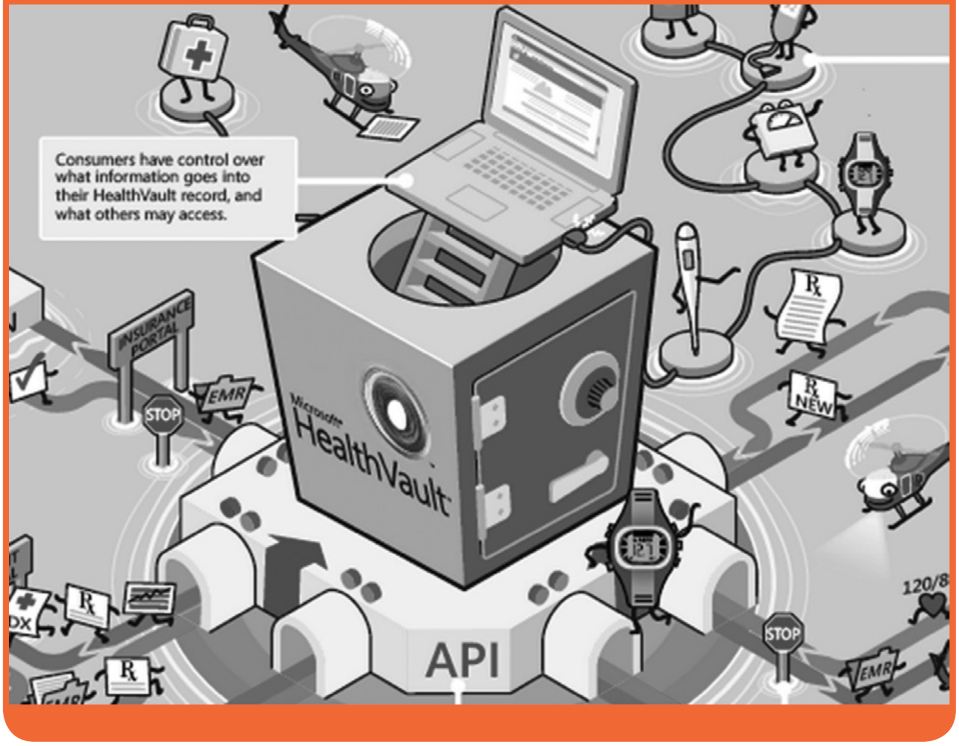
Backup
Save each kind of important data and files scheduled and automatically!

Synchronizer
Synchronize local folders or FTP folders scheduled and automatically!

An overview of the IT-specific *Top Ten Big Data Security and Privacy Challenges* is provided in the report of the same name by the Cloud Security Alliance – including the Fujitsu and HP Labs – of November 2012.

Another focus is that of the Digital Vault. This kind of vault exists in different sorts and sizes, from simple consumer applications – by British Telecom, for example – to patented vault technology by suppliers such as CyberArk, which has been especially developed to come up to the level of the best secured bank vaults.

A concrete application, in line with the new Electronic Health Record, is Microsoft HealthVault. In this type of personal vault individuals can store their health-related information, update it, link it to devices and share it with medical professionals, the drugstore, insurers and other parties without any problem.


Consumers have control over what information goes into their HealthVault record, and what others may access.
INSURANCE PORTAL
STOP
EMR
Microsoft HealthVault
API
℞
℞ NEW
120/8
DX

Privacy by Design is the use of technical and organizational measures in information systems to avoid invasions of people's personal privacy. If information systems are inherently privacy-friendly, this considerably adds to a sustainable information society.

But, by and large, the report by TNO and TILT explains, the protection of privacy encompasses all activities and measures aimed at the regulation of access to the individual in a situational, relational and informational sense. So this extends beyond the protection of personal data or, in other words, data protection.

At the end of the day, the protection of privacy aims to protect or enhance people's personal autonomy and to reduce their vulnerability to material damage, discrimination and stigmatization, for example, as much as possible. Moreover, privacy is not only meant to protect individuals. The values on which privacy is based also have important social and libertarian dimensions.

Privacy enables people to arrive at individual views and preferences without outside interference. In this way, privacy adds to the multiformity and creativity of society and to the protection and enforcement of the democratic constitutional state. All this according to TNO and TILT.

3.4 E-privacy-related challenges

The view of TNO and TILT is a legitimate, albeit very idealistic one of the e-privacy discussion. A more concrete emphasis on *Trustworthy Social eCommerce* is found on Eprivacy.com, expressed by Philippe Coueignoux. In his analysis "ePrivacy, What's at Stake?" Coueignoux explains that IT and Internet-related internal fraud, external fraud and explicit privacy issues all cause breaches of confidence that directly put a spanner in the works, as he puts it, of *Economic Activity & Individual Business Valuation*. Coueignoux provides the following useful classification of five e-privacy-related themes that he observes among *Liabilities and Vulnerabilities in the Information Age.*

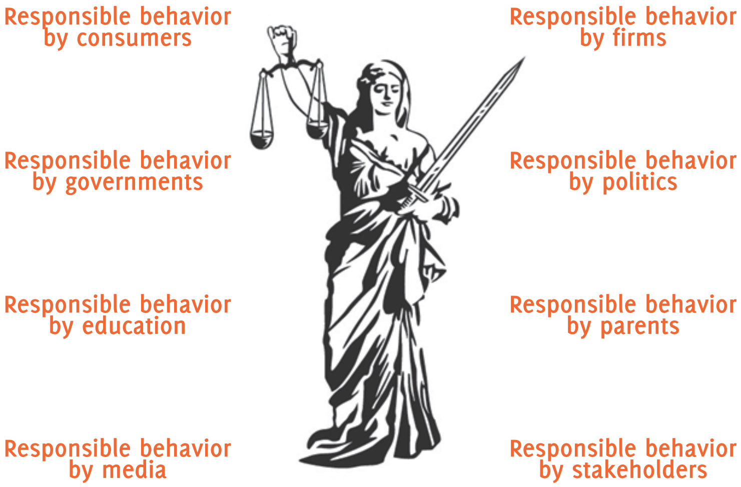
Overview of online privacy issues

1. *Identity:* identity theft, credit fraud, ambush marketing
2. *Ownership:* medical records, marketing campaigns, international data & Safe Harbor (see section 4.6), surveillance, viral marketing
3. *Location:* searching and matching data
4. *Defense (the good side):* protecting, storing, using, distributing and recommending digital information
5. *Offense (the dark side):*
   - stealing time from receivers: spamming, manipulating search results
   - blocking access: denial of service, censorship
   - falsifying the context: copying, plagiarism and forgery, advertising fraud

A recent suggestion by Coueignoux to presidents Barack Obama and Herman van Rompuy is to tax the economic use of privacy; it should be done progressively and separately from the continued enforcement of e-privacy legislation. Coueignoux's partly technological Privacy & Security by Design solution dovetails with the economic value that personal data has in the age of the Internet.

3.5 Responsible behavior as core value

Responsible behavior is the core value of all ethical-legal themes. On account of its fluidity, this is certainly true of the protection of personal digital data on the Internet. A non-limitative, generic list of kinds of behavior displayed by various stakeholders, with legislation and regulation, jurisdiction and jurisprudence in the centre – preferably internationally harmonized or uniformized – is shown next:


Responsible behavior by consumers
Responsible behavior by firms
Responsible behavior by governments
Responsible behavior by politics
Responsible behavior by education
Responsible behavior by parents
Responsible behavior by media
Responsible behavior by stakeholders

All the possibilities and means at the disposal of Justice for the purpose of its legislative, executive/enforcing and judiciary powers are truly impressive, but we still have a long way to go before it is all realized in actual practice. Ideally, Privacy by Design and Security by Design are at the basis of all efforts in the context of privacy and security.

First and foremost, Privacy & Security by Design involves building in privacy protection by means of Privacy-Enhancing Technologies (PETs), beginning with the system design. Apart from the technical micro-level, the principle should also be effective on an organizational meso-level and legal macro-level. The aim of Privacy & Security by Design is twofold: secure privacy-friendly system designs, and a sustainable information society in day-to-day practice.

More information can be found in the recent report entitled *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* by Ann Cavoukian, the Canadian Information and Privacy Commissioner, which is also discussed in the conclusion.

4 Legislation in a state of flux

4.1 We ourselves are the enemies of privacy 44
4.2 Throwing away my privacy for 50 cents 44
4.3 Privacy no longer the social standard 46
4.4 Privacy & Security: the new drivers of Brand, Reputation and Action 46
4.5 Effectively formulating and rationalizing plans 48
4.6 Guidelines of the OECD, e.g. 49
4.7 Privacy Impact Assessment (PIA) 51

4.1 We ourselves are the enemies of privacy

The American Supreme Court Judge Alex Kozinski finds it hard to understand that we tend to blame others for our loss of privacy. After all, why do that if we refuse to take our own privacy seriously? Today's exhibitionistic behavior is making it increasingly difficult for American judges to stand up for privacy. It is day-to-day practice, in conjunction with other factors, that decides how the government and the judicature deal with it and, if that practice implies exhibitionism, then that change of standards is a fact.

In a Twitter world where the police can ping us on a smartphone in the wink of an eye, an increasing number of people regard this simply as a matter of having more followers. This was Kozinski's tongue-in-cheek observation at the Stanford Law Enforcement Symposium 2012 on "privacy and its conflicting values":

> *The idea that law enforcement can now ping your cell phone and find out exactly where you are at any time, with no probable cause and no judicial supervision, is greeted with a big collective yawn. In a Twitter world where people clamor for attention, having the police know your whereabouts just increases your fan base.*

Join the conversation

PbD question 6
Is everything you have arranged with regard to privacy clear to the stakeholders, and do they know what will happen in concrete cases?

http://bit.ly/vintR3Q6

4.2 Throwing away my privacy for 50 cents

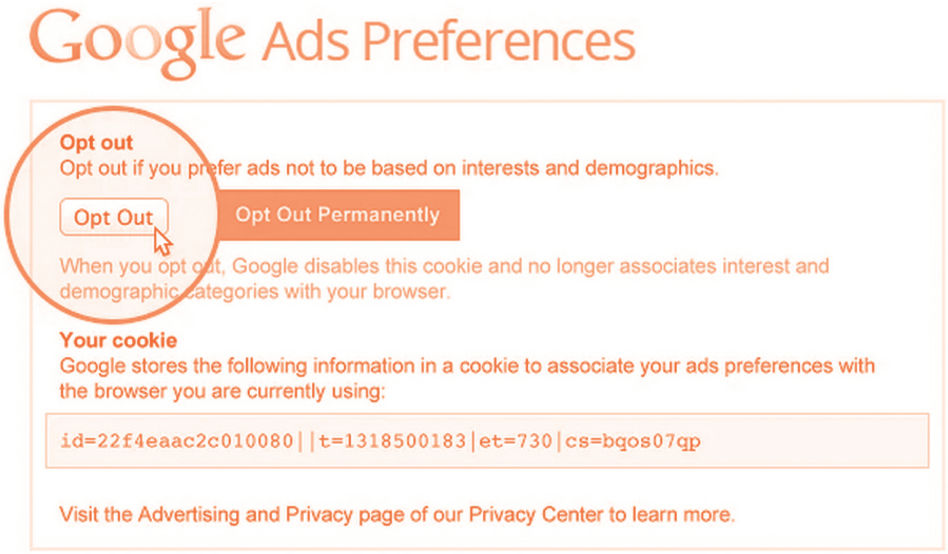
What is our privacy worth to us? A fifty-cent discount on a 7.50 cinema ticket is an excellent online exchange for our telephone number or e-mail address. This appears from the *Study on Monetizing Privacy* by ENISA, the European Network and Information Security Agency of early 2012.

Evidently we do not care much about divulging personal information. Three-quarters of Europeans increasingly regard it as a fact of life. Over 40% of European Internet users say they are asked to supply more data online than is strictly necessary, but just do it all the same. This was revealed by the study *Attitudes on Data Protection and Electronic Identity in the European Union*, carried out in late 2010.

In the following year, Facebook doubled its revenue from advertising to almost 4 billion dollars. This concerns first, second and third-party cookies, which keep a close track of our online behavior and make capital out of it. Consciously supplying information is one thing, but being followed without being fully aware of it is a much larger issue in the personal data concern. For this reason, a stringent opt-in cookie law was introduced in the Netherlands in June 2012, which was liberalized again just before the end of the year in accordance with the intended European standard. For, apart from privacy, entrepreneurship and innovation are also considered to be of paramount importance, not least in economically hard times.

More and more people are saying that we should just forget all about our privacy; after all, something like privacy simply no longer exists in this age of the Internet, just as little as "intellectual property," for example. Perhaps it does not really matter either way because, analogous to this, most companies are scared to death of the reputational damage that might be caused if it turns out that customers are being closely scrutinized without their knowledge, just to optimize the companies' profits.

Large-scale abuse of data on the basis of a few simple cookies is grossly exaggerated and a rigid opt-in rule would be disastrous for entrepreneurship. The prevailing view is that we have to deal with articulate consumers nowadays and, if they are properly informed and the possibilities to opt out are pointed out to them, that is the most attractive economic situation for all parties.



Google Ads Preferences

Opt out

Opt out if you prefer ads not to be based on interests and demographics.

When you opt out, Google disables this cookie and no longer associates interest and demographic categories with your browser.

Your cookie

Google stores the following information in a cookie to associate your ads preferences with the browser you are currently using:

```
id=22f4eaac2c010080||t=1318500183|et=730|cs=bqos07qp
```

Visit the Advertising and Privacy page of our Privacy Center to learn more.

4.3 Privacy no longer the social standard

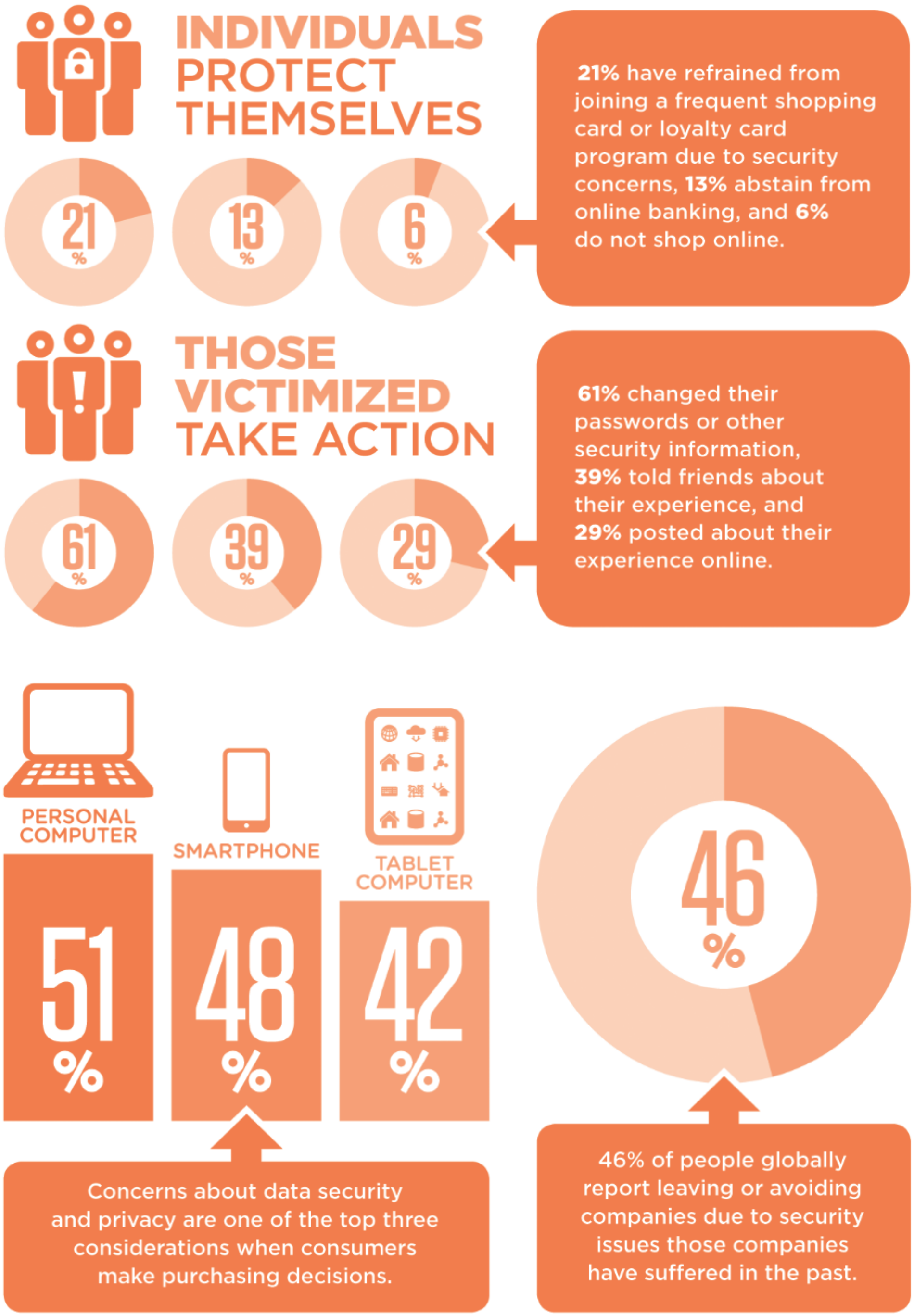
The first one to repudiate the relevance of the digital privacy discussion was Scott McNealy, the then CEO of Sun Microsystems. "You already have zero privacy – get over it," he said in 1999 when Jini was introduced: software intended to link a large number of different devices. For example – as is perfectly normal today – making a photograph that is uploaded automatically to a newspaper via the Internet, so that it ends up in newspaper stands all over the world the same day.

One decade later, in early 2010, Mark Zuckerberg, the CEO of Facebook, took a similar stand in an interview with TechCrunch, by arguing that privacy was no longer the social standard. "When we started Facebook in my room at Harvard seven years ago," said Zuckerberg, "we wondered if people would put information online at all. But in a few years' time the standards entailed in privacy have changed completely. And we are simply moving with the times."

Kozinski, ENISA, McNealy and Zuckerberg arrive at the same conclusion from different perspectives: in the past decades, and years even, the views of privacy have undergone a tremendous change, which is why, apart from standards and values, the rules and regulations are likewise moving with the spirit of the times.

4.4 Privacy & Security: the New Drivers of Brand, Reputation and Action

The latter is perfectly obvious from Edelman's info diagram (shown below), which has been drawn up on the basis of a survey in 2012 among 4050 individuals from 7 different countries. Edelman calls privacy and security the "New drivers of the brand." Privacy must become a core task for every organization. Almost half of all the consumers interviewed state they tend to avoid companies that have failed to protect data properly. The fact that security breaches, for example, may go viral in an instant and generate a tremendous amount of negative publicity is one of the reasons for organizations to engage with these new competencies with great enthusiasm.



INDIVIDUALS PROTECT THEMSELVES

21% have refrained from joining a frequent shopping card or loyalty card program due to security concerns, **13%** abstain from online banking, and **6%** do not shop online.

THOSE VICTIMIZED TAKE ACTION

61% changed their passwords or other security information, **39%** told friends about their experience, and **29%** posted about their experience online.

Concerns about data security and privacy are one of the top three considerations when consumers make purchasing decisions.

46% of people globally report leaving or avoiding companies due to security issues those companies have suffered in the past.

If much commotion is made about a privacy breach at all, the organization in question will usually have a quick and easy statement prepared that it considers to be in line with prevailing regulation and standards. By and large, privacy matters are considered very seriously in economic activities. But – on account of its high-profile Big

Brother issues – privacy is a field of increasing controversy and (hyper)sensitivity, and there are many people who are all too eager to sound the alarm.

There is no denying that weak security of systems, far-reaching powers for authorities, a hodgepodge of obsolete laws and regulations, actions by groups such as WikiLeaks and Anonymous, cybercrime and cyberwarfare etcetera strongly determine the sentiment with regard to e-privacy and data protection. It would be wrong, however, to indiscriminately continue this negative sentiment in the context of the day-to-day privacy practices of organizations engaged in business activities.

In the context of the information society, the Surveillance Society and Big Data, everything that concerns privacy is very much in a process of flux at the moment, while measures are further refined and focused. For example, the idea is that the European Guideline, on which national governments currently base their own privacy laws and regulations, will be replaced by a stringent regulation in 2015; in short, by a universally applicable European law. Such uniformization is advisable in order to create an economic *level playing field*.

However, without a concrete case, the question as to what is and what is not allowed with regard to privacy can hardly be answered satisfactorily. But even if there is a case, there are many comparative assessments and pros and cons in the balance. In addition, it is difficult to explain current legislation while it also displays so many gaps, according to the opinions of various experts we consulted for this research report.

4.5 Effectively formulating and rationalizing plans

When one has commercial plans, the following points are vital:

1. They have to be formulated as precisely as possible and, ideally, one should be able to indicate where one would like to be in, say, five years' time.
2. One has to demonstrate on the basis of well-reasoned arguments why the intended actions are fair and socially justified in relation to the focus group of customers, staff, prospects and suspects, for instance.
3. Subsequently it can be decided in consultation whether or not there is an acceptable legal form available. The target group should at least be informed of the plans (obligation to provide information) and there should be no gap between rhetoric and reality.
4. Transparency is of vital importance and anything reminiscent of discrimination and applying double standards, like *dual pricing*, must be avoided.
5. Explicitly asking for permission is only required in the case of serious matters such as health and criminal law, etc.

6. Big Data practices, like gathering personal information from a variety of sources and subsequently drawing conclusions as a result, e.g., segmentation, must be explained carefully.
7. *Straight-through processing* – in general, processing data without human intervention is not allowed.

4.6 Guidelines of the OECD, e.g.

A practicable and universal first point of departure for the protection of privacy and data is the OECD guidelines of 1980, summarized at http://oecdprivacy.org. These *OECD Privacy Principles*, eight in all, concern respectively:

- *Collection Limitation:* data must not be gathered haphazardly or illegally, and, if applicable, they should be gathered with the knowledge or permission of the party concerned.
- *Data Quality:* the accuracy of the data must be guaranteed.
- *Purpose Specification:* it must be clear what the data will be used for.
- *Use Limitation:* the use of the data must be limited.
- *Security Safeguards:* the security of the data must be guaranteed.
- *Openness:* it must be perfectly clear which data are being collected and what will be done with them.
- *Individual Participation:* during the entire process of gathering and using the personal data etc., the individual must be actively involved and offered easy access, so that the person in question is informed adequately and is in a position to take action.
- *Accountability:* the "data controller" is responsible for the compliance with these eight Fair Information Practice Principles (FIPS).

These principles can be consulted in detail and in their context on the IT Law Wiki (http://itlaw.wikia.com/wiki/The_IT_Law_Wiki).

All in all, this is perfectly in tune with the European view of privacy. The American *Consumer Privacy Bill of Rights* of February 2012 (officially: *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*) contains an attachment in which America's own Fair Information Practice Principles (FIPS) are compared with those of the OECD among others.

A 119-page document of the European Commission of January 2012 presents the so-called "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)." The idea is that this proposal will come into force in 2015.

At the annual European Data Protection and Privacy Conference in 2012, the American ambassador William Kennard said that the EU's new data protection rules threaten the co-operation between the European and American police and judiciary, because hundreds of investigation regulations that are functioning perfectly well would have to be adjusted.

Apart from the above OECD guidelines, the OECDprivacy.org website mentions another three privacy frameworks: the *Asia-Pacific Economic Cooperation (APEC) Privacy Framework*, the *United States Department of Commerce Safe Harbor Privacy Principles*, and the *Generally Accepted Privacy Principles* (GAPP). The worldwide trend with regard to privacy and security regulation is one of harmonization, uniformization and standardization.
The US-EU Safe Harbor treaty aims to help American organizations meet the EU rules with regard to the protection of personal data. It includes checklists, self-certification and a workbook. The following seven Safe Harbor principles are central:

- *Notice* – Individuals must be informed that their data are being collected and about how they will be used.
- *Choice* – Individuals must have the ability to opt out of the collection and onward transfer of the data to third parties.
- *Onward Transfer* – Transfers of data to third parties may only take place to other organizations that follow adequate data protection principles.
- *Security* – Reasonable efforts must be made to prevent loss of collected information.
- *Data Integrity* – Data must be relevant and reliable for the purpose they were collected for.
- *Access* – Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- *Enforcement* – There must be effective means of enforcing these rules.

That looks good, but after two negative reviews by the European Union in 2002 and 2004, Galexia expressed the following opinion in 2008:

The growing number of false claims made by organisations regarding the Safe Harbor represent a new and significant privacy risk to consumers.

The OECD rules mentioned above are officially called the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The complete text can be found in the documents under the heading “Information security and privacy,” a topic in the section “Internet economy” on the website.

4.7 Privacy Impact Assessment (PIA)

To keep the theme of privacy and security practical, a *Privacy Impact Assessment* (PIA) can be made to clarify in advance the risks inherent in the implementation of plans. The British Information Commissioner’s Office, for example, has such a *PIA Handbook* and distinguishes the following nine steps:

- identifying interested parties
- initial assessment of privacy risks
- decision as to the extent of PIA
- mapping out privacy risks
- consulting interested parties
- making proposals for acceptance
- moderating or avoiding risks
- checking compliance
- planning a review.

The review examines the actions undertaken as well as the effects, which may result in a more extensive or even new PIA.

Conclusion

Privacy is a concept that dates from the fifteenth century, but as early as the first century BC, Publilius Syrus said that we should not associate with “friends” who shout our private matters from the rooftops. This is an excellent message in this era of social media, which just goes to show that privacy issues have existed since time immemorial, and are closely connected with the individuality that is typical of every rational human being.

Everyone likes to exercise discrimination when it comes to his or her privacy. Traditionally the mine and thine and our private domain are at stake, but digital privacy is a particularly ambivalent matter. If we have been branded by information systems as being less creditworthy, for example, this may have long-term effects, as practice has shown many times. And this gives a nasty flavor to the concept of digital DNA.

Privacy scandals have a long half-life: we tend to nurture our suspicion. Only too often have we lapsed into the same old mistakes, somehow or other. Statistically speaking, it reminds us of the wise men who are unable to answer all the fool’s ques-

Join the conversation

PbD question 7
Confidence is essential in privacy issues. Do you highlight the interaction with individuals to a sufficient degree?

http://bit.ly/vintR3Q7

tions or remove his fundamental distrust. Anything that is in the public eye tends to take root, not least in the absence of systematic clarity.

Nowadays, everyone is very much aware that privacy, technology and regulation form the triad that should be able to provide sufficient clarity and certainty to generate a better socio-economic digital world. An integral approach to Privacy by Design will have to create a basis for trust so that we may eventually reap the fruits of a digital economy.

The development of Big Data and its applications emphasizes the urgency of an effective approach, with reference to both the side of fear and that of hope, of ambition. With all the widespread complexity and doubt, it is becoming more and more manifest that only a concrete and integral Privacy by Design approach can provide a solution. But due to the unending series of privacy breaches, anxiety and distrust will continue to dominate.

This is a constant existential factor, as privacy is rooted in the individual's solitude. Rationally it culminates in the methodical doubt of Descartes, philosopher of the Enlightenment: distrust characterizes our attitude to life. Actually, Big Data gain for everyone presupposes a mathematical argumentation, but there is no such thing and if there was, only a minority would understand it.

The fundamental trade-off character of privacy prevents a consensus. But this is exactly where the fair play of economic potential starts for everyone. As has been noted at the beginning of this report, digital privacy is the capacity to negotiate social relationships by controlling access to personal information.

Laws, policies and technology increasingly structure people's relationships with social institutions, authorities and one another. This offers new challenges but also opportunities with regard to privacy. For this reason, a new conceptual framework needs to be created for the analysis of privacy policies on the one hand and the design and development of data processing systems on the other.

The reasoning in this context is as follows: Big Data is a reality; it is extremely valuable, but at the same time nourishes unease with relation to privacy. A proper balance needs to be created between organizations and individuals. Privacy by Design, Privacy-Enhancing Technologies, standardized legislation in addition to the corresponding responsible behavior constitute the integral approach that should enable Big Data gain for everyone.

The Introduction to this report outlines how the personal information economy works. A variety of organizations are engaged in collecting data about us all that can end up virtually anywhere, through different types of information brokers: with banks, marketers, media, government authorities, legal organizations, individuals, legal instances and employers. Only organizations that exclusively collect privacy-neutral information of fewer than 5,000 individuals a year and do not share it with third parties in any way whatsoever fall outside the scope of this ecosystem, according to the American Federal Trade Commission. All other parties need to pay serious attention to the implementation of Privacy by Design and to simple options for consumers, and they must continue to demonstrate transparency towards the market.

As privacy, data protection and personal information represent such a high economic and relational value, organizations need to operationalize Privacy by Design on the basis of the following seven basic principles:

1 *Privacy by Design means that you take proactive and preventive action: not reactive – no repairs afterwards*
Try to anticipate so-called *privacy-invasive* events as much as possible and, first and foremost, try to prevent them. Do not wait until a privacy invasion presents itself.

2 *Privacy guarantee needs to be the default setting*
You aim to guarantee maximum privacy for individuals and make sure that personal information is safe and secure in any IT system and business operation.There should be no need for individuals to worry about this or to take action.

3 *Privacy needs to be embedded in the design*
Privacy requirements need to be an integral part of the design and the architecture of IT systems and business operations. Privacy is an essential component of the functionality that is supplied.

4 *Go for full functionality: no poor trade-off but a clearly positive balance*
Address the legitimate privacy interests and objectives as a win-win situation. Avoid apparent opposites such as privacy versus security and demonstrate that they may well occur simultaneously.

5 *Solutions need to be totally conclusive and unequivocal: end-to-end security at all times*
Security is a central element. One of the aspects of data protection is that all data can be destroyed securely at the end of a process or other lifecycle, or at any desired moment.

6 Ensure full visibility and transparency: openness is your leitmotiv
It should be perfectly clear to stakeholders what exactly is going on with regard to all business operations and IT solutions. It should be possible for any party involved to check this at any time.

7 Deal with privacy respectfully: particularly by focusing on the individual
Strong privacy defaults, a timely explanation of what is going on, and user-friendly options for individuals are indispensable to a relationship based on mutual trust. The interaction is decisive in this context.

These principles bear upon the core of any organization: digital technology, design and infrastructure plus the operation itself. They have been further elucidated and elaborated in the report entitled *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* of December 2012, complete with actions and responsibilities in the organization on the part of management, software architects, developers, business-line owners and owners of applications. It also includes specific examples, such as the healthcare and energy sectors and, in the field of technology, camera surveillance and near-field communication (tap & go).

Literature and illustrations

Agre, P.E. & M. Rotenberg (1997): *Technology and Privacy: The New Landscape*, http://polaris.gseis.ucla.edu/pagre/landscape.html

Alessandro Acquisti, A. (2010): "The Economics of Personal Data and The Economics of Privacy," http://www.oecd.org/sti/interneteconomy/46968784.pdf, http://www.heinz.cmu.edu/~acquisti/papers/acquisti_privacy_economics.ppt

Alvaro, A. (2012): *Lifecycle Data Protection Management: A contribution on how to adjust European data protection to the needs of the 21st century*, http://www.alexander-alvaro.de/wp-content/uploads/2012/10/Alexander-Alvaro-LIFECYCLE-DATA-PROTECTION-MANAGEMENT.pdf

American Library Association (ca 2005): Privacy Tool Kit / Checklist of Basic Questions about Privacy and Confidentiality, http://www.ala.org/offices/oif/iftoolkits/toolkitsprivacy/guidelinesfordevelopingalibraryprivacypolicy/guidelinesprivacypolicy

Article 29 Data Protection Working Party (2013): *European data protection authorities publish their joint opinion on mobile apps*, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130314_pr_apps_mobile_en.pdf

Asimov, I. (1951): *Foundations*

Bradbury, R. (1951): *Fahrenheit 451*

Burkert, H. (1997): "Privacy-Enhancing Technologies: Typology, Vision, Critique," http://books.google.nl/books?id=H2KB2DK4w78C&pg=PA125

Bygrave, L.A. (2002): "Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place," http://folk.uio.no/lee/publications/PETS_speech.pdf

Cavoukian, A. (2009): "Privacy by Design: The 7 Foundational Principles," http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Cavoukian, A. (2012): *Operationalizing Privacy by Design. A Guide to Implementing Strong Privacy Practices*, http://privacybydesign.ca/content/uploads/2012/12/operationalizing-pbd-guide.pdf

Cavoukian, A. & J. Jonas (2012): *Privacy by Design in the Age of Big Data*, http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf

CEN: European Committee for Standardisation (2010): Data Protection and Privacy Download Pages, http://www.cen.eu/cen/Sectors/Sectors/ISSS/CWAdownload/Pages/DPPCWA.aspx

Center for Internet and Society PET wiki: http://cyberlaw.stanford.edu/wiki/index.php/PET

Clarke, R. (1995-2013): Dataveillance & Information Privacy, http://www.rogerclarke.com/DV

Clarke, R. (2001): "Introducing PITS and PETS: Technologies Affecting Privacy," http://www.rogerclarke.com/DV/PITSPETS.html

Clinton, W.J. & A. Gore (1997): "A Framework voor Global Electronic Commerce," http://clinton4.nara.gov/WH/New/Commerce/read.html

Cloud Security Alliance (2012): *Top Ten Big Data Security and Privacy Challenges*, https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Top_Ten_v1.pdf

Computers, Privacy & Data Protection (2013): "Reloading Data Protection," http://www.cpdpconferences.org/sponsors.html

Coueignoux, P. (2006): "Liabilities and Vulnerabilities in the Information Age," http://www.eprivacy.com/lectures/toc.html

Coueignoux, P. (2012): “The Privacy Tax. Open letter to Barack Obama and Herman van Rompuy,” http://www.cawa.fr/the-privacy-tax-article005879.html

Coueignoux, P. (2013): ePrio, trustworthy social eCommerce, http://eprivacy.com

Cyberspace Law and Policy Centre (2008): *Distinguishing PETs from PITs: Developing technology with privacy in mind*, http://www.cyberlawcentre.org/ipp/publications/papers/ALRC_DP72_Technology_final.pdf

Daniel P. (2013): “Abine’s DeleteMe app review: deal with personal info databases from the comfort of your phone,” http://www.phonearena.com/news/Abines-DeleteMe-app-review-deal-with-personal-info-databases-from-the-comfort-of-your-phone_id38722

De Wereld Draait Door (2012): “Doorstart EPD: Wilna Wind en Alexander Klöpping,” http://dewerelddraaitdoor.vara.nl/media/197890

Department of Defense (2013): Personally Identifiable Information Course Module, http://iase.disa.mil/eta/pii/pii_module/pii_module/index.html

Department of Health, Education and Welfare (1973): “The Code of Fair Information Practices,” http://epic.org/privacy/consumer/code_fair_info.html

Department of Homeland Security (2011): *Handbook for Safeguarding Sensitive Personally Identifiable Information At The DHS*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf

Diploma of Information Technology, Knowledge Management (2012): “Types of Privacy,” http://toolboxes.flexiblelearning.net.au/demosites/series4/411/content/privacy/types_of_privacy.htm

Duhigg, C. (2012): “How Companies Learn Your Secrets,” http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Edelman (2012): “Privacy & Security: The New Drivers of Brand, Reputation and Action. Global Insights 2012,” http://edelmaneditions.com/wp-content/uploads/2012/03/Data-Security-Privacy-Infographic_Final.png

Electronics Weekly (2010): “Electroon #9 - ‘Computer says No’” (1960), http://www.electronics-weekly.com/blogs/electronics-weekly-blog/2010/09/electroon-9---computer-says-no.html

Ellis Smith, R. (2004): *Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, http://www.privacyjournal.net/_center_ben_franklin_s_web_site__privacy_and_curiosity_from_plymouth_rock_to_the_3087.htm

ENISA (2012): *Study on monetising privacy: An economic model for pricing personal information*, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy

European Commission (2010,2011): *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Europese Commissie (2012): *Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming)*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:NL:PDF http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Export.gov (2012): U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, http://export.gov/safeharbor

Fair Information Practice Principles, FIPS (1973, 1980), http://simson.net/ref/2004/csg357/handouts/01_fips.pdf

Federal Trade Commission (2012): *Fair Information Practice Principles*, http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Federal Trade Commission (2012): *Marketing Your Mobile App: Get It Right from the Start,* http://business.ftc.gov/documents/bus81-marketing-your-mobile-app

Federal Trade Commission (2012): *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers*, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

Fielder, A. (2013): "European Parliament committees threaten wholesale destruction of privacy and data protection rights," https://www.privacyinternational.org/blog/european-parliament-committees-threaten-wholesale-destruction-of-privacy-and-data-protection

Foremski, T. (2011): "SFcurators: Our Public, Private, And Secret Lives…," http://www.siliconvalleywatcher.com/mt/archives/2011/07/sfcurators_our.php

Frankfurter Allgemeine (2011): "Der deutsche Staatstrojaner wurde geknackt," http://www.faz.net/aktuell/chaos-computer-club-der-deutsche-staatstrojaner-wurde-geknackt-11486538.html

Galexia (2008): "The US Safe Harbor – Fact or Fiction?," http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction-Recommen.html

Garfinkel, S. (2001): *Database Nation. The Death of Privacy in the 21st Century*

Gerber, B. (2009, 2010): OECD Privacy Principles, http://oecdprivacy.org

Gorodyansky, D. (2013): "It's Data Privacy Day: 3 Things You Must Do," http://www.inc.com/david-gorodyansky/3-ways-to-go-all-out-this-data-privacy-day.html

Greenberg, A. (2008): "The Privacy Paradox," http://www.forbes.com/2008/02/15/search-privacy-ask-tech-security-cx_ag_0215search.html

Hagel, J. (2012): "The Rise of Vendor Relationship Management," http://edgeperspectives.typepad.com/edge_perspectives/2012/06/the-rise-of-vendor-relationship-management.html

Hamlin, K. (2012): "Personal Data List in Mind Map Form," http://www.identitywoman.net/personal-data-list-in-mind-map-form

Hirschleifer, J. (1979): *Privacy: Its Origin, Function, and Future*, http://www.econ.ucla.edu/workingpapers/wp166.pdf

HP Laboratories (2011): *Privacy-Enhancing Technologies: A Review*, http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf

Huffington Post (2010): "Facebook's Zuckerberg Says Privacy No Longer A 'Social Norm'" (video), http://www.huffingtonpost.com/2010/01/11/facebooks-zuckerberg-the_n_417969.html

Human Rights Council (2012): Resolution A/HRC/20/L.13: The promotion, protection and enjoyment of human rights on the Internet, http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf

Huxley, A. (1932): *Brave New World*

Information Commissioner's Office (1998): "Data protection principles," http://www.ico.gov.uk/for_organisations/data_protection/the_guide/the_principles.aspx

Information Commissioner's Office (2013): "Privacy impact assessment (PIA)," http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

Internationaal privacykader (2013): http://www.cbpweb.nl/Pages/ind_wetten_int.aspx

IT Law Wiki (2013): "Privacy-Enhancing Technologies" [incl. UK ICO & EU], http://itlaw.wikia.com/wiki/Privacy%E2%80%90enhancing_technologies

IT Law Wiki (2013): “The IT Law Wiki,” http://itlaw.wikia.com/wiki/The_IT_Law_Wiki

Johnson, H. (2013): “The Application Privacy, Protection, and Security (APPS) Act of 2013,” http://apprights-hankjohnson.house.gov/2013/01/apps-act.shtml

Kennard, W.E. (2012): “Remarks by U.S. Ambassador to the EU, William E. Kennard, at Forum Europe’s 3rd Annual European Data Protection and Privacy Conference,” http://useu.usmission.gov/kennard_120412.html

Koorn, R.F. & J. ter Hart (2011): “Privacy by Design: From privacy policy to privacy-enhancing technologies,” http://www.compact.nl/artikelen/C-2011-0-Koorn.htm

Kozinski, A. (2012): “The Dead Past,” http://www.stanfordlawreview.org/online/privacy-paradox/dead-past

Kuner, C. et al. (2012): “The Challenge of Big Data for Data Protection,” http://idpl.oxfordjournals.org/content/2/2/47.extract

Kuneva, M. (2009): Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling, http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm

Lee, F. (2006): *An Investigation of Privacy Tradeoff on the Internet*, http://citebm.business.illinois.edu/twc%20class/project_reports_spring2006/privacy%20issues/lee/internet_privacy_fei.pdf

Lynley, N. (2013): “A Palantir Founder Suggests His Startup Is Worth About $8 Billion,” http://blogs.wsj.com/digits/2013/01/16/a-palantir-founder-suggests-his-startup-is-worth-about-8-billion

Mackay, S. (2012): “‘Apps’ and Big Data and Privacy – An Oxymoron?,” http://ediscoverytalk.blogs.xerox.com/2012/12/10/apps-and-big-data-and-privacy-an-oxymoron

Magenta Advisory (2012): “Wise use of consumer data enables to improve companies’ performance and creates possibilities for new services and solutions,” http://www.magentaadvisory.com/2012/09/12/wise-use-of-consumer-data-enables-to-improve-companies-performance-and-creates-possibilities-for-new-services-and-solutions/

Microsoft (2012): *Differential Privacy for Everyone*, http://www.microsoft.com/en-us/download/details.aspx?id=35409

Microsoft HealthVault: http://www.healthvault.me/, https://www.healthvault.com/nl/nl, http://www.microsoft.com/health/en-us/products/Pages/healthvault.aspx

Microsoft HealthVault Ecosystem: http://www.netsoft-usa.com/images/img_medtracker_HealthVaultFuture.png

MozillaWiki (2011): Privacy Icons project (beta release), https://wiki.mozilla.org/Privacy_Icons

Mulligan, D. (2012): “Bridging the Gap between Privacy and Design,” http://www.law.berkeley.edu/14542.htm

Nader, R. (1965): “Unsafe at Any Speed,” http://www.nndb.com/people/788/000023719/

National Institute of Standards and Technology (2010): *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

OECD (2013): “Information security and privacy,” http://www.oecd.org/sti/interneteconomy/informationsecurityandprivacy.htm

Olsson, M. (2012): “NSA Building A $2 Billion Quantum Computer Artificial Intelligence Spy Center,” http://mind-computer.com/2012/05/13/nsa-building-a-2-billion-quantum-computer-artificial-intelligence-spy-center

Öman, S. (2004): *Implementing Data Protection in Law*, http://www.scandinavianlaw.se/pdf/47-18.pdf

OpenLearn (2012): “Secret or sharing? Play our Privacy Game,” http://www.open.edu/openlearn/privacy

Orwell, G. (1948): *1984*

Out-law.com (2012): “Smart meter technology is privacy intrusive,” http://www.out-law.com/en/articles/2012/january-/smart-meter-technology-is-privacy-intrusive-researchers-claim

Packard, V. (1964): *The Naked Society*, http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=3842&context=fss_papers

Pfanner. E. (2013): “French Tax Proposal Zeroes In on Web Giants’ Data Harvest,” http://www.nytimes.com/2013/02/25/technology/french-tax-proposal-zeroes-in-on-web-giants-data-harvest.html

PISA Consortium (2003): *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents*, http://www.cbpweb.nl/downloads_technologie/pisa_handboek.pdf

Pratt, W.F. (1979): *Privacy in Britain*, http://books.google.nl/books?id=GDjNgEgw2fgC

“Privacy & Free Speech: It’s Good for Business,” http://www.dotrights.org/business/primer

Privacy by Design (2013), http://www.privacybydesign.ca

Privacy Impact Assessment .nl (2013): Privacy Quick Scan, http://privacyimpactassessment.nl/QuickScan.html

Privacy Rights Clearinghouse (2013): “Empowering Customers. Protecting Privacy.” Fact Sheet 12: Checklist of Responsible Information-Handling Practices, https://www.privacyrights.org/fs/fs12-infohandling.htm, https://www.privacyrights.org/about_us.htm

Privacy, Technology and the Law, http://www.judiciary.senate.gov/about/subcommittees/privacytechnology.cfm

Rand, A. (1943): *The Fountainhead*

Reyburn, S. (2012): “ACT debuts the App Privacy Icons,” http://www.insidemobileapps.com/2012/10/04/act-debuts-the-app-privacy-icons/

Rosen, J. (2012): “The Right to Be Forgotten,” http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

Rousseau, J-J. (1754): *Discourse on the Origin and Basis of Inequality among Men*

RT, Russia Today (2012): “NSA refuses to disclose its links with Google,” http://rt.com/usa/nsa-epic-foia-court-413

RTL Z (2013): “Privacy op internet niet goed beschermd,” http://www.rtl.nl/components/financien/rtlz/nieuws/2013/03/privacy-op-internet-niet-goed-beschermd.xml

Rubinstein, I. (2011): *Regulating Privacy By Design*, https://www.privacyassociation.org/media/pdf/knowledge_center/Regulating_privacy_by_design.pdf

Rubinstein, I. (2012, 2013): *Big Data: The End of Privacy or a New Beginning?*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659

Schoen, S. (2009): “What Information is ‘Personally Identifiable’?,” https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable

Searls, D. (2010): “Do we have to ‘trade off’ privacy?,” http://blogs.law.harvard.edu/vrm/2010/09/19/do-we-have-to-trade-off-privacy

Sengupta, S. (2012): “Building an Iconography for Digital Privacy,” http://bits.blogs.nytimes.com/2012/11/19/building-an-iconography-for-digital-privacy

Smith (2012): “Digital privacy in the big data era: Microsoft’s data protection keynote,” http://www.networkworld.com/community/blog/digital-privacy-big-data-era-microsofts-data-protection-keynote

Sogeti VINT (2012, 2013): vier Big Data-onderzoeksnotities, http://vint.sogeti.com/bigdata

Solove, D.J. (2006): *A Taxonomy of Privacy*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622

Solove, D.J. (2011): *Nothing to Hide: the False Trade-off between Privacy and Security*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1827982

Solove, D.J. & P.M. Schwartz. (2011): *Privacy Law Fundamentals*, https://www.privacyassociation.org/media/pdf/publications/PLF_TOC.pdf, “Chapter 1: An Overview of Privacy Law in all its varied types and forms and a timeline with key points in the development of privacy law,” https://www.privacyassociation.org/media/pdf/publications/PLF_Chap_1.pdf

South Australian Law Reform Institute (2012): *Computer says no. Modernisation of South Australian evidence law to deal with new technologies*, http://www.law.adelaide.edu.au/reform/downloads/issues-paper-1-computer-says-no.pdf

Spiegel, Der (2012): “Surfing for Details: German Agency to Mine Facebook to Assess Creditworthiness,” http://www.spiegel.de/international/germany/german-credit-agency-plans-to-analyze-individual-facebook-pages-a-837539.html

Strahilevitz, L.J. (2004): *A Social Networks Theory of Privacy*, http://www.law.uchicago.edu/files/files/230-ljs-privacy.pdf

Surveillance Studies Network (2006): *A Report on the Surveillance Society for the Information Commissioner*, http://www.surveillance-studies.net/?page_id=3

Szoka, B. (2009): *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, http://ftc.gov/os/comments/privacyroundtable/544506-00035.pdf

Tavani, H. & D. Vance (1996): “Chapter 4.3 Computers and Privacy,” http://home.aisnet.org/displaycommon.cfm?an=1&subarticlenbr=633

Tene, O. & J. Polonetsky (2012): *Big Data for All: Privacy and User Control in the Age of Analytics*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364

Tene, O. & J. Polonetsky (2012): “Privacy in the Age of Big Data: A Time for Big Decisions,” http://www.stanfordlawreview.org/online/privacy-paradox/big-data

TNO, TILT (2011): *Trusted Technology. Een onderzoek naar de toepassingsvoorwaarden voor Privacy by Design in de elektronische dienstverlening van de overheid*, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/12/05/trusted-technology-een-onderzoek-naar-de-toepassingsvoorwaarden-voor-privacy-by-design-in-de-elektronische-dienstverlening-van-de-overheid.html

Tompor, S. (1994): “The Credit Report from Hell,” http://www.recordnet.com/apps/pbcs.dll/article?AID=/19940801/A_NEWS/308019321

TrendLabs (2012): *Be Privy to Online Privacy*, http://about-threats.trendmicro.com/ebooks/be-privy-to-online-privacy/files/assets/downloads/publication.pdf

Upshure, R.E.G. et al. (2001): “The privacy paradox: laying Orwell’s ghost to rest,” http://www.ncbi.nlm.nih.gov/pmc/articles/PMC81333

Verenigde Naties (1948): Universele Verklaring van de Rechten van de Mens, artikel 12, http://www.un.org/en/documents/udhr/index.shtml#a12

Vitaliev, D. (2011): “Data Protection and Privacy,” http://dmitri.vitaliev.info/data-protection-and-privacy

VNO NCW (2011): Brief: Kabinetsnotitie Privacy met o.m. Privacy Ouick Scan (PIA), http://www.vno-ncw.nl/SiteCollectionDocuments/Brieven/brief11-11507.pdf

Warren, S. & L. Brandeis (1890): "The Right to Privacy," http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Westin, A.F. (1967): "Privacy and Freedom," http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr

Westin, A.F. & M.A. Baker (1972): *Databanks in a Free Society. Computers, Record-keeping, and Privacy*

Wet bescherming persoonsgegevens (2013), http://www.cbpweb.nl/pages/ind_wetten_wbp.aspx

White House, The (2012): *Consumer Data Privacy in a Networked World. A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Wolfensberger, D.R. (2006): "Congress and the Right to Privacy," http://www.wilsoncenter.org/sites/default/files/privacy-essay-drw4.pdf

World Economic Forum (2011): *Personal Data: The Emergence of a New Asset Class*, http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

World Economic Forum, Boston Consulting Group (2013): *Unlocking the Value of Personal Data: From Collection to Usage*, http://www.weforum.org/issues/rethinking-personal-data

Zamyatin, Y. (1924): *We*

Privacy: great – but what's the next step...?

1. For an overall picture of digital privacy for your business, see for example the Checklist of Responsible Information-Handling Practices from the US Privacy Rights Clearinghouse. Another good starting point is the Checklist of Basic Questions about Privacy and Confidentiality from the Privacy Tool Kit (sub IV) of the American Library Association. Instead of "library," please read "information" or "data." Also, the Data Protection and Privacy Download Pages on the website of the European Committee for Standardisation CEN are rich sources of information.
2. Chapter 4 of this research report suggests that you make a *Privacy Impact Assessment* (PIA).
3. The structural development of managing privacy as an economic catalyst is called *Privacy by Design* (PbD). There is a high degree of consensus concerning the benefit of this possible solution. Privacy by Design has been operationalized in the conclusion of this report on the basis of seven recommendations. To guide you in that direction, these seven recommendations for Privacy by Design have also been put in the margin as questions throughout the research report.

(please continue on the back cover)

About Sogeti

Sogeti is a leading provider of professional technology services, specializing in Application Management, Infrastructure Management, High-Tech Engineering and Testing. Working closely with its clients, Sogeti enables them to leverage technological innovation and achieve maximum results. Sogeti brings together more than 20,000 professionals in 15 countries and is present in over 100 locations in Europe, the US and India.

About VINT

It is an arduous undertaking to attempt to keep up with all developments in the IT field. State-of-the-art IT opportunities are often very remote from the workings of core business. Sources that provide a deeper understanding, a pragmatic approach, and potential uses for these developments are few and far between. VINT, the Sogeti Trend Lab, provides a meaningful interpretation of the connection between business processes and new developments in IT.

In every VINT publication, a balance is struck between factual description and the intended utilization. VINT uses this approach to inspire organizations to consider and use new technology.

Privacy: great – but what's the next step...?

(Privacy by Design (PbD) – continued from page 62)

http://bit.ly/vintR3Q1

PbD question 1
Have you ever had anything to do with privacy issues? The Privacy by Design (PbD) approach is expressly intended to prevent this.

http://bit.ly/vintR3Q2

PbD question 2
Is personal information in your IT systems secure by definition, so that no one needs to worry about this?

http://bit.ly/vintR3Q3

PbD question 3
Are privacy requirements an integral part of the design and architecture of your IT systems and business practices?

http://bit.ly/vintR3Q4

PbD question 4
How do you deal with privacy versus security? Do you think they can exist in perfect harmony?

http://bit.ly/vintR3Q5

PbD question 5
In the context of data protection, do you also believe that it must be possible to destroy information definitively at a given moment?

http://bit.ly/vintR3Q6

PbD question 6
Is everything you have arranged with regard to privacy clear to the stakeholders, and do they know what will happen in concrete cases?

http://bit.ly/vintR3Q7

PbD question 7
Confidence is essential in privacy issues. Do you highlight the interaction with individuals to a sufficient degree?

Participate in our Big Data discussion at www.sogeti.com/vint/bigdata/questions

SOGETI

VINT | Vision ● Inspiration ● Navigation ● Trends