Corien Prins

INTRODUCTION

Today, in our already information-intensive society, tailored and individualized services and platforms appear to gain unprecedented popularity. New technologies such as mobile location-based services, Radio Frequency Identification (RFID), smartcards, ambient technologies and biometrics support an ever greater capturing of customer and user information and allow for tailored services to the individual’s needs and desires. Prospects to private as well as public sector organizations in applying these and other services are numerous: they range from the improvement of quality of service delivery and customer relations, to getting to know your customer and behavioural marketing, cost reduction and a more efficient achievement of organizational goals (e.g. profit, policy effectiveness), as well as effective enforcement of legal rights (e.g. copyright). In addition, a growing number of individual people benefit from new technology-based facilities. Individuals themselves e.g. create an unprecedented rich digital source of information by teaming up with like-minded people to create social network sites and other web 2.0 applications. And, with mobile location-based services, people can trace other individuals with similar preferences that are present within the same geographical space of about 30 metres.

Insight knowledge about individual customers, patients or citizens provide commercial as well as public sector organizations with highly valuable information. Some organizations even join forces with groups of individuals. Illustrative is the well-known industry-patient partnership patientslikeme.com.1 Personalized information also allows companies to address a large number of people on an individualised basis at the same time; not only within the territorial vicinity of the company or organization, but even globally. Web-based personalisation is one of the fastest growing segments of the digital economy, having spawned a multimillion-dollar industry.2

---

Some argue we find ourselves on the eve of a new type of market. In describing the characteristics of the new ‘collaborative economy’, Yochai Benkler claims that peer production and other forms of collaboration reverse earlier market strategies by breaking down the barrier between the market self and the social self.3

In short, personalization facilitated by technology seems to be an important, if not inevitable tool and strategy for private and even public organizations to deploy all kinds of individual-centric activities and services. The proliferation of personalized services, however, also triggers concerns. For the development may have profound effects on information and transaction relationships between individuals, organizations and/or communities in our society. At the heart of these concerns and effects is the very issue of user identification. It raises privacy problems as well as concerns with respect to inclusion and exclusion. Personalization may be a threat to a user’s privacy because it provides companies and organizations with a powerful instrument to know in detail what an individual wants, who he or she is, whether his or her conduct or behaviour shows certain symptoms, and so forth. Also, personalization may be disturbing because it facilitates the selected provision to specific users only and may thus diminish certain preferences, differences and societal values. In a worst-case scenario, personalization may have larger societal and political consequences when it would shape the overall movement of information and expression within society. A discussion on how to react to the emergence of online personalization, should therefore not be limited to a discussion on privacy implications and how to protect individual data. Instead, it should be a discussion about essential interests such as autonomy, control, transparency and (digital) diversity.

In this contribution, I will be concentrating on some key effects of the emergence and growing popularity of online personalized services. Issues that will be addressed are privacy, inclusion and exclusion as well as transparency and control. As will become clear from this discussion, personalized services and the creation of digital identities are closely related. We should therefore recognize the crucial role of digital identities in the further development of online services. Based on an analyses of the afore-mentioned issues, I will be arguing that the focus of the discussion on enhanced privacy protection mechanisms should therefore move away from entitlements of single data. What we need are instruments to enhance the visibility of and our knowledge about how personal data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes. A discussion of privacy protection in an information society characterized by personalized services should therefore be a discussion about protecting our digital identities instead of our individual personal data.

---

3 Benkler 2009.
As said, the development of personalization services will have important effects on privacy. What raises problems in relation to privacy is first the potential for further use and sometimes abuse of the detailed and rich knowledge on individuals. Connecting and (re)selling data sources has become a highly profitable business and certain companies may compromise users’ privacy for profits. In the meantime, studies have shown that consumers and citizens are under certain conditions particular about the type of information they are willing to provide in return for personalized content. However, most consumers hardly understand how personalization technologies actually work and have ample opportunity for control over the dissemination of their personal or behavioural information. Various personalization services deploy hidden instruments to track and trace users and thus consumers are usually not aware of their data and preferences being collected.

With the growing importance of personalization services, it is clear that ownership rights in personal data and individual user profiles become the key instrument in realizing returns on the investment. As early as October 2003, Jupiter Research study found that to develop and deploy a personalized website can cost four or more times than operating a comparable dynamic website. Thus, a healthy business model for personalized services requires that the key asset, i.e. the personalized information, ‘belongs’ to the organization that has configured its system to allow users to perform personalization. But who then owns and thus may control personal data? Who owns our personal Google-profile or any of the profiles created in one of the many popular social networks? At first glance, day-to-day practice appears to indicate that the data controller, i.e. the organization that collected the data for personalization purposes, holds some sort of property right in these data. Several bankruptcy cases in the early years of this decennium have shown that databases containing personal data and consumer profiles are a highly valuable asset. With the at that time downturn in the e-business market, various companies decided to sell their customer data as a means of generating cash flow and silencing creditors. In many other situations, customer lists and databases appeared a highly valuable asset as well. Large amounts of personal data changed hands or ‘ownership’, as part of merger-
acquisitions, reorganizations and other strategic company movements. More recently, the takeover of various companies that have made their business in the online world testifies of what is at stake when it comes to the acquisition of subscriber, user and customer lists. Companies may even actually believe that they have ownership rights in the personal data compilations because the law itself offers indications for such a position. In addition to protection under the regime of trade secrets, businesses that have invested in the collection and compilation of personal data are granted exclusive rights under the European Directive on database protection.

In line with the debate on ownership in personal data, commentators have argued that it is the individual who should own the information about himself and decide how the data are being used and by whom. In this view, ownership and control of identity must belong to the person identified. In the 1990’s, creating property rights in personal data was thought to be a plausible way of securing interests in our modern technology-based era. Academics in the area of law and economics, argued that by granting individuals a property right in their personal data, they could sell or license their data and thus determine how much information they share with others and at what price. In looking at privacy as a problem of social cost, commentators felt that the accepted conception of privacy was an ineffectual paradigm and that, if we want strong privacy protection, we must replace it with the more powerful instrument of a property right. By vesting a property right in individuals, businesses would be forced to internalize the costs associated with the collection and processing of personal data.

At present, businesses gain the full benefit of using personal information, but do not bear the societal costs: personal data can usually be collected for free, and with the advent of new technologies, it has become much easier and cheaper to gather and use data of individuals. Once companies have to internalize the societal costs associated with using personal data, they would perhaps be less inclined to gather and compile personal data than they currently do. This, in turn, would enhance levels of privacy. Moreover, placing some cost burden on processors and users of personal data promotes greater respect for individual dignity than requiring individuals to purchase their privacy against a default rule of no-privacy. Thus, the costs are no longer only borne by those individuals who both desire privacy and can afford it, but instead by society as a whole.

Others however warned for what they called the failure of licensing and thus the failure of a property-based protection model. Individuals will gladly consent to certain personalized uses of their data or user profile. Or they

---

7 Gauthronet 2001.
9 Laudon 1996.
10 Sholtz 2000.
12 Cohen 2000, p.1390.
may not wish to consent or are reluctant to consent, but are nevertheless forced to consent because without use-rights the company is not willing to provide certain services. In other words, bargaining seems impossible or consumers have no effective choice in the matter. To do any good, the property right might have to be inalienable and waivable only in certain limited circumstances (comparable to the moral rights under intellectual property law).

But even if data subjects would be willing to permit the use of their personal data, actually licensing all the necessary data will be costly, inconvenient, and time-consuming which in the end could mean that companies no longer have the adequate incentive to offer personalized services.

**Technology as a solution**

More recently, an alternative proposal that has been suggested: to use technology to create and sustain the conditions for personalized choices of the data used. Certain digital technologies, such as privacy enhancing technologies and ‘technologies of identity’ as described by Phil Agre, make it possible to prevent personal data from being collected at all. Also, technology can provide the means for encoding personal data with detailed information about restrictions on use, exchange and further processing. In line with this argument, Cohen contended that the same technologies that enable personalized distributed rights-management in the area of copyrighted works might enable the creation of privacy protection that travels with data – obviating the need for continual negotiation of terms, but at the same time redistributing “costs” away from individuals who are data subjects.

Zittrain, describing the use of personal data in the medical arena, made the claim that ‘trusted’ architectures (i.e. hardware and software that take note of various entitlements to personal data they store and automatically enforce those entitlements) could help negotiate the allocation of use rights to personal data. Personalization techniques could thus balance the legitimate interests of companies and organizations who wish to use data and the interests of individuals who ‘produce’ these data for the very reason that personalization techniques increase the ability to uphold and enforce rights and obligations. The inclusion in techniques of certain default rules that restrict the collection of personal data without individual consent could provide individuals with a tool to control information about themselves, permitting them to waive it, but setting default contract terms that help shape the licensing practice that may thus develop.

---

14 Agre 1997.
16 Zittrain 2002.
Thus, in line with what has been contended by Samuelson, this approach would not focus on granting individuals a law-based property right in their personal data, but rather on restricting or conditioning the use and alienability of these data once obtained by a specific compiler. By now, several open standards for so-called identity management have been developed, based on ownership models and rooted in the concepts of the individual’s autonomy and sovereignty.17

Inclusion and Exclusion

A consideration closely related to the use of personal data and privacy protection is the inclusion and exclusion of individuals when it comes to certain personalized services. Clearly, the deployment of personalization applications will facilitate the widespread monitoring of what people read, view, or listen to. By using personalization services their proprietors will potentially have what Philip Agre referred to ten years ago as “God’s-eye view of the world.”18 To the extent that personalization applications allow the user to be tracked easily and thoroughly, it is a simple matter to limit the scope of certain facilities to a tightly controlled group of consumers. For example, personalization services will facilitate the selected provision of access to certain services only to consumers who live in preferred zip codes, or have certain levels of income. Also, personalization services seem well-suited to choose who will be allowed to view or read a particular work and who will not. But personalization is not only about inclusion or exclusion of certain services. It will also facilitate price-discrimination – that is, proprietors of services can ask different consumers to pay different prices.

Is this inclusion or exclusion good or bad? It could be argued that inclusion or exclusion is economically useful, because it will do a better job of getting the right information (commercial as well as public sector information) to the right persons. In the absence of personalization techniques, organizations must make wasteful investments in distributing information to consumers of whom they do not know whether they appreciate this information. Thus, techniques that facilitate inclusion and exclusion may be especially useful to accommodate the varying preferences of consumers and citizens. As such, personalization is a good way to achieve an efficient market. Personalization, further, provides an efficient and effective tool with which companies can monitor who is granted access to certain works and who is not. By using personalization techniques, content-producers obtain control over the uses of a variety of legally protected works and the techniques will thus allow providers to choose who will be allowed to view or read particular works. The control facilitated by personalization techniques e.g. will

---

18 Agre 1999.
increase the copyright owners ability to uphold and enforce their copyrights. Also, one could argue that personalization techniques would offer consumers a better privacy perspective because it provides them with the power to restrict the collection of personal data.

Of course, one might argue that inclusion and exclusion of (access to) certain services is essentially nothing new and as such there is nothing bad to it. Today, consumers and citizens behaviour is also predetermined by their attachment to a group, their cultural or societal position or predisposition, etc. What is different however with the new dimension of personalization services is that it may force individuals into restraining, one-dimensional models, based on the criteria set by technology and of those who own and apply the technology. With commercial personalization services, the myriad of individual differences is reduced to one or a few consuming categories. And on the basis of these few categories everything has been said about their preferences, character, life-style, and so forth.

But also from other perspectives it seems disturbing that personalization offers the ability to diminish certain preferences, differences and values. For example an exclusion of access to and the use of information and copyrighted works (music, books, films) puts the values of free speech and information under pressure. What is more, personalization may have larger societal and political consequences when it would shape the overall movement of information and expression within society. Free citizens are the cornerstone of democratic constitutional societies. In an ultimate scenario personalization services could put cultural and social diversity at stake: one political or religious message is to dominate the whole discourse. In other words, personalization may have serious consequences when it means that behaviour is manipulated, freedom of self-determination and personal autonomy is limited and societal freedom is eroded. Personalization as such is nothing new, since inclusion and exclusion are part of our daily life. However, the control facilitated by personalization services may potentially have (serious) consequences for freedom of speech, freedom of consuming and freedom of conscience, as well as the public interest of cultural and political diversity.

A discussion on the pros and cons of personalization from the inclusion and exclusion perspective could be held along the lines of the concepts of autonomy and paternalism. The concept of autonomy has been described in many different terms and values. Feinberg described autonomy as: “The kernel of the idea of autonomy is the right to make choices and decisions... put compendiously, the most basic autonomy right is the right to decide how to live one’s life.” Thus, to act as an autonomous individual, freedom and respect in making choices is essential. To be able to make choices, an individual:

---

19 Van der Hof & Prins 2008.
20 Feinberg 1986.
must be free from unwarranted interference by others (non-interference);

must be able to make choices (capacity);

must be able to make meaningful choices, i.e. understanding the relevant information (informed).  

Of course, unchallenged exercises of autonomy are not tolerated in all situations. For example, a person will not be entirely free to make his own choice in a situation in which the exercise of such choice will directly harm third persons. Also, for certain reasons third persons (private as well as public bodies and persons) may decide what is best for others. This concept of paternalism is based on the presumption that in certain situations people, organizations or governments may and even must decide for others what is in their best interest.

The key challenge with the new opportunities of personalization will in the end be to find a balance between autonomy and paternalism. But what is crucial in realizing this balance is that individuals will at least be given the instruments to enhance the visibility of and their knowledge about how their personal data are used and combined, on the basis of what they are typified, by whom and for what purposes. In line with Nissenbaum’s theory of contextual integrity, “it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances.”

The key problem we face with the advent of personalized techniques is, quoting Mireille Hildebrandt: “an abundance of co-relatable data and the availability of relatively cheap technologies to construct personalized knowledge out of the data, create new possibilities to manipulate people into behaviour without providing with adequate feedback of how their data have been used (…) (T)his may lead to major shifts in power relations between individual citizens on the one hand and commercial or governmental organizations on the other. The crucial issue is not abuse, but the fact that we have no effective means to know whether and when profiles are used or abused”.

This brings us to a third consideration of importance for an analysis of privacy and personalization: transparency and quality.

---

21 Laurie 2002.
24 Hildebrandt 2008.
Digital Diversity: Protecting Identities Instead of Individual Data

TRANSPARENCY AND QUALITY

Both concepts reveal themselves in different aspects and on different levels of personalized services; however, these concepts are also correlated to a large extent in the sense that both contribute to each other. At a practical level several requirements can be discussed when it comes to transparency and quality. First of all, transparency with respect to the personalization process itself is of importance, including information as to how the personalization process works, the different configuration options or features which are included in the service etc. Moreover, the purpose(s) for which personal data and related information (e.g., log-in information, transaction histories, and localization information) is used within the personalized service or beyond should be transparent to users. Users should also be aware of the way in which their personalized identity is created and used by the personalized service provider (e.g. what methods are used to create identities and in what context(s) are personal data used and viewed). In addition, users should be informed of the way in which personal data can be accessed, reviewed and updated and the security of this process. Furthermore, users should know if and how (e.g., by sending an e-mail to a clearly specified address) they can restrict or object to (commercial) use of their personal and other data. Such information can, e.g., be provided in a privacy statement on the website of the service provider. Privacy statements should be complete and easy to access and understand. From a quality perspective it is also important that the security of personal and other data is adequate and that usability of security and more specifically authentication mechanisms is optimized. Usability across different personalized services can, for instance, be addressed by implementing what is called single sign-on authentication mechanisms.

Transparency also demands that users can assess the objectivity, quality and reliability of information provided to them through the personalized process. More than one business or other organization may be involved in providing users with a variety of personalized services and information and, particularly, where there is a lock-in situation in which service providers determine the information to be received by individual users, users should be able to trace the origin of information in order to be (better) able to determine the quality, objectivity and reliability of such information.25

PERSONALIZATION AND IDENTIFICATION

Having discussed the implications of personalization for privacy, inclusion/exclusion and transparency/quality, we finally touch upon the core challenge of this new development, i.e. the implications of personalization for

the way our lives are typified and our identities are constructed by means of the new technological application.

As was mentioned, a key feature of personalization is that individuals are given new ways to present and profile themselves – depending on the specifics of the context – in certain roles or ‘identities’. The earlier-mentioned ‘patientslikeme’ initiative is only one of many examples that show that people act as a certain type of citizen, consumer, patient, voter, et cetera. The thus growing importance of the context-specific concept of online identity raises challenging new questions as regards the role as well as status of identity and identification. To what extent does the concept of ‘online identity’ get a different meaning compared to identity construction in offline relationships? Where exactly in social networks lie the boundaries between online identities and a person’s ‘own’ or ‘real’ identity? When exactly, i.e. given what conditions, may a certain fragmented or segmented aspect of a person’s identity be considered an adequate representation of the ‘real’ person behind that identity?26

If online personalization will become in part tantamount to the online identity of a person, then this state of affairs may raise the question who may control the use of the data behind this identity as well as the identity itself. Can an online identity be owned and if yes, in whom should such ownership be vested? Finally, new means of self-presentation also raises questions related to the reliability of identities and the implications of possible fraud with identities. To what extent can users ‘play’ with their online identity or virtual ‘reputation’, use their online reputation as a certain type of ‘security’, mislead organizations with a claimed online identity, et cetera?

Another way to consider the relationship between the public domain and the commodification of personal data is by focusing not so much on the individual data, but on the effects of the present-day technologies, in particular the almost limitless surveillance capacities of new technologies, such as location-based systems, radio frequency identifiers (RFIDs) and online personalization instruments. In a sense, these surveillance techniques require that we shift our attention from individual sets of personal data toward the statistical models, profiles and the algorithms with which individuals are assigned to a certain group or ‘identity’. For these models and algorithms are privately owned, and thus unavailable for public contestation. But the interests of personal data protection seem to require that they are made known to the public and thus are part of the public domain. Let me discuss this point in some more detail.

Our behaviour in the ‘public domain’ is increasingly monitored, captured, stored, used and analyzed to become privately-owned knowledge about people, their habits and social identity. Indeed, the term personal data protection may loose its significance once we acknowledge this trend toward a commodification of identities and behaviour. It is this trend that is lacking in

26 Leenes 2008.
Digital Diversity: Protecting Identities Instead of Individual Data

the present debate on personal data protection. Personal data are not used and processed anew and in isolation each time a company acquires a set of personal data. In contemporary society, ‘useful’ information and knowledge goes beyond the individual exchange of a set of personal data. In ‘giving’ his or her personal data to a certain organization, the individual does not provide these data for use in an ‘objective’ context. Today, the use and thus ‘value’ of personal data cannot be seen apart from the specifics of the context within which these data are used. Processing of personal data occurs within, and is often structured by, social, economic and institutional settings, as is e.g. shown by Phillips in his analysis of the implications ubiquitous computing developments.27

Thus, the question is not so much whether personal data are processed. They always are and will be, whether for legitimate or unlawful purposes. It is an illusion to think that vesting a property right in personal data will limit the use of personal data. Rather, the problem is how personal data are processed, in what context, and towards what end. Therefore, the focus of the discussion should move away from entitlements of single data. What we need are instruments to enhance the visibility of and our knowledge about how personal data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes.

A similar suggestion is for other reasons made by academics in the area of marketing.28 This is a much more fundamental issue which cannot be tackled by vesting for example a property right in individual data. To illustrate this argument, I would like to point towards another new technology-based development: ubiquitous computing environments. Ubiquitous computing will create a context-aware environment in which, by means of the coordinated use of databases, sensors, micro-devices and software agents, numerous systems scans our environment for data and serve us with particular information, based on certain notions about what is appropriate for us as unique individual persons given the particulars of daily life and context. Some thus argue that ubiquitous systems will to a large extent structure and determine our daily life, mediating our identity, social relations and social power. Not only will our homes and working offices become public places, but our social identities as well.

Conclusion

Given not only the development of personalization but also other developments in the area of ‘pervasive’ computing, the discussion about protecting personal data must become a discussion about how individuals are typified (upon what social ontology, with what goal?) and who has the instruments

and power to do so. In this sense, personal data protection is not about something (i.e. personal data) that can be owned. It has everything to do with position, social ordering, roles, individual status and freedom. Therefore, protection of personal data in our present-day society assumes the capability to know and to control about how our identities are constructed. It requires the availability of instruments to enable awareness of the context in which personal data are used and to monitor the data-impression that individuals are exhibiting to others.\(^{29}\) In other words, the discussion on the future of privacy protection must be a discussion on whether, and to what extent, the statistical models, profiles and algorithms that are used to generate knowledge about our individual behavior, social and economic position, as well as personal interests, are transparent and controllable. And in the end, it is precisely this discussion that is essential in the interest of societal values such as autonomy, control, transparency and (digital) diversity. Almost ten years ago, Vedder advocated the introduction of the new concept of ‘categorical privacy’. This concept is largely based on the concept of individual privacy, but including privacy as regards information that is no longer identifiable to persons, because such information may still have possibly negative consequences for group members.\(^{30}\)

But perhaps the time has come to take it one step further: to call for the recognition of a sui generis right, namely the ‘right to identity’.\(^{31}\) By making explicit and ‘legal’ the value of identity, this new basic right would provide a better-equipped instrument to balance the private and public interests at stake than only the rights to privacy or liberty. Others, however, believe that the negative aspect of freedom – the maintenance of legal, administrative, political and ethical opacity – is and should remain quintessential. Issues pertaining to ‘identity’ or to be protected by normative prohibitions of interferences such as foreseen by privacy and some aspects of data protection law, but also by freedom of conscience and speech, physical integrity, etc.\(^{32}\) It is too early to decide what road to follow. What is however clear is that the focus of the discussion on the future of privacy protection should move away from entitlements of single data. What we need are instruments to enhance the visibility of and our knowledge about how personal data are used and combined, on the basis of what data individuals are typified, by whom and for what purposes. A discussion of privacy protection in a world of internet of things, ambient intelligence, social networks and convergence should therefore be a discussion about protecting our virtual identities and the interests behind this concept, instead of our individual personal data.

\(^{29}\) Nguyen & Mynatt 2002.
\(^{30}\) Vedder 2000.
\(^{31}\) Prins 2007; De Hert 2008.
\(^{32}\) Gutwirth 2009.
References

Agre 1997

Agre 1999

Benkler 2009

Cohen 2000

Dworkin 1988

Feinberg 1986

Gauthronet 2001

Gutwirth 2009

De Hert 2008

Hildebrandt 2008

Van der Hof & Prins 2008

Laudon 1996

Laurie 2002

Leenes 2008
Lemley

Nguyen & Mynatt 2002

Nissenbaum 2004

Phillips 2005

Prins 2007

Samuelson 2000

Sholtz 2000

Vedder 2000

Vedder & Wachbroit 2003

Volokh 2000

Zittrain 2000

Zwick & Dholakia 2004
Introduction

During one of the many animated lunchtime discussions at eLaw@Leiden, the topic was the notion of a technological Singularity. Singularity is a theoretical point in the future of mankind where we will be able to create smarter-than-human-intelligence through the use of technologies such as artificial intelligence and nanotechnology.\(^1\) Being a techno-optimist myself, I feel this is an exciting prospect. Professor Schmidt however, saw cause for great concern instead of ground for optimism.

Much like Asimov, who noted that science gathers knowledge faster than society gathers wisdom, Schmidt argues that society will be unable to cope with the problems of smarter-than-human intelligence. Apart from the obvious problems of a smarter-than-human mind setting itself to nefarious purposes, and the possibility of an immense (digital) divide between normal humans and ‘smarter-than-humans’, professor Schmidt argues that Singularity may also threaten the legitimacy of our law systems.\(^2\)

While in general I feel Singularity (if it ever occurs) will be beneficial for mankind, I must agree with professor Schmidt that it will pose serious problems for the working and legitimacy of our legal system(s). In this article I shall look at a specific cause for concern: the protection of the right to privacy in (near) Singularity societies. But before I discuss the problem statement of this article, I shall first describe more in depth what we mean by a technological Singularity.

Countdown to Singularity

Technological Singularity is a concept introduced by science fiction author Vernor Vinge and expanded on by many authors and researchers, most notably Ray Kurzweil.\(^3\) In examining the history of human evolution and technology, Vinge and Kurzweil observed that the pace of technological development is growing at an exponential rate. They argue that in the near future

---

\(^{1}\) Kurzweil 2005.
\(^{2}\) Schmidt 2009.
some thirty to forty years from now) our technology will have evolved so far, that we will have the technological capabilities to create smarter-than-human intelligence. This point in time is called Singularity.

Singularity will come about as a result of the convergence of Nanotechnology, Biotechnology, Information technology and insights from Cognitive sciences (NBIC). In particular, the advent of ‘strong’ artificial intelligence will enable us to surpass our current physical and mental boundaries. For instance by using nanobots we can heal our bodies and slow the aging process, by using sophisticated brainscanning techniques we can map our brain functions for replication in a computer, and through brain-machine interfaces we can enhance our brains with technology. These ideas have led ‘Singulatarians’ such as Vinge and Kurzweil to believe that we will be either surpassed by a smarter-than-human intelligence or gradually transform into a post-human species. This idea of post- or transhumanism is as appealing as it is disturbing. Though it is my personal opinion that the controversial theories set forth by Kurzweil on self-replicating nanobots, the emergence of strong artificial intelligence and possibly even the ability to copy our conscience into a machine, are plausible, we cannot hope to verify or falsify them at this point in time. Nonetheless, since Singulatarian ideas seem grounded in science, they deserve careful study, most importantly because they will pose significant ethical and societal challenges.

Unfortunately, it is impossible to discuss the ethical and societal implications of Singularity for the simple reason we cannot begin to comprehend what the advent of smarter-than-human intelligence will mean. Actually, this is the reason why Vinge called the advent of smarter-than-human intelligence ‘the Singularity’ in the first place. Much like Singularity at the heart of a black hole, where the normal rules of physics no longer apply, we cannot see beyond the technological Singularity point because we are not as smart as post-humans and are thus enable to predict or comprehend their actions. Therefore, we will be unable to draw up an ethical framework with accompanying rules and regulations. What we can do however, is take a few steps back on the road to Singularity and focus on what I would like to call ‘near Singularity’ issues. While it is possible that Singularity will happen abruptly and unexpectedly (what is called ‘the hard take off’ scenario), I feel it is more likely that there will be steady improvements in technology, which in the end will lead to Singularity (what is called the ‘soft take off’ scenario).^4

This does not mean that near Singularity issues likely to arise in a soft take off scenario will be any less profound. On the contrary, the technological changes and their societal effects will have a profound impact on our notions of autonomy, justice, equality, property, privacy et cetera. In this article I will focus on the possible effects of near Singularity technologies on the privacy of individuals. In particular I shall focus on the use of these technologies for surveillance purposes and discuss the following problem statement:

---
^4 A view supported by Kurzweil, see: http://www.acceleratingfuture.com/people/blog/2007/the-Singularity-a-hard-or-soft-takeoff/. 

Privacy and Singularity: little ground for optimism?

What are the effects on near-Singularity technologies on the privacy of individuals and how can we maintain the right to privacy in the face of these technologies?

To (try and) answer this problem statement I shall start by describing the impact of technology on privacy and how the law has responded to these challenges. Apart from a historical description I shall also describe how privacy will change in the coming years as a result of the ubiquitous computing paradigm and the rise of NBIC technologies. From there I shall describe what risks the use of these technologies may entail. From there I shall suggest possible solutions to counter the negative effects of these technologies.

A brief history of privacy ... and its end

Research into primitive societies suggests that mankind has always needed some measure of privacy. Through history, there has been a need for privacy in every society. However, what 'privacy' exactly entailed within these societies, is markedly different from our current notion of privacy. This is due to the fact that privacy, as a social institution, is defined by the realities of a particular place and time in history. Changing attitudes towards the body, the house, the family, work and the State have always influenced the right to privacy. In the last hundred years or so, the rapid pace of technological development has been the driving force behind changing attitudes towards privacy. It is my opinion that in the next twenty years, technology will completely blur the boundaries between the public and the private, prompting us to rethink fundamentally our current notions and ideas about privacy.

1890-1928: cameras and wiretapping
At the end of the 19th century and the beginning of the twentieth century technological developments such as the invention of the snapshot camera and the increasing use of telecommunication networks (and the ability to tap these networks), gave rise to questions about a right to privacy. Justices Warren and Brandeis made the first explicit reference to a right to privacy in their renowned article The Right to Privacy: The Implicit Made Explicit. Dismayed as they were by the practices of the gossip press which used “new inventions and business methods” to invade the “sacred precinct of private and domestic life”, Warren and Brandeis set out to explore the possibility and origin of a right to privacy. Warren and Brandeis came to the conclusion that the right to privacy formed part of the inviolate personality and saw it as: “the next step that must be taken for the protection of the person, and for securing to the individual... ...the right ‘to be let alone’.”

---

5 Westin 1984.
7 Warren & Brandeis 1890.
8 Warren & Brandeis 1890.
It was the same Brandeis who in his dissenting opinion in the case of *Olmstead versus the United States* insisted on a person’s right to private communications. In *Olmstead* the United States Supreme Court held that tapping a phone line outside someone’s house is not a violation of the right to privacy since no physical search or seizure is conducted. The decision in *Olmstead* came to be known as the ‘trespass doctrine’. The trespass doctrine linked privacy to a physical place (viz. the house), rather than to the communication itself. It was not until *Katz v. the United States* that the trespass doctrine was reversed. In this decision, the Supreme Court held that the legitimacy of interference into the personal sphere is determined by an individual’s ‘reasonable expectation of privacy’. The Court held that a person has a right to privacy with regards to his private conversations and therefore wiretapping is prohibited without a prior warrant.

1960-2010: the rise of information technology

The next technological development that had a major impact on privacy was the invention of the computer. In the course of some fifty years, our society has been transformed from an industrial society into an ‘information society’. This transformation has been spearheaded by the development of the personal computer and the internet. The ‘digital revolution’ has had a profound impact on privacy and the conceptualisation of privacy as a human right.

The rise of automated recordkeeping in the sixties and seventies gave rise to a growing worry that automated data processing would pose a threat to basic human liberties. In the Netherlands for instance, there was active protest against the 1971 census (volkstelling), which was seen as an infringement of privacy. In 1973 the United States Department of Health, Education, and Welfare drafted a seminal report titled *Records, Computers and Rights of Citizens* that contained a *Code of Fair Information Practices*. These Fair Information Practices consisted of five basic principles to which every data processing party should adhere. They are: 1) no secret recordkeeping, 2) a duty to inform data subjects, 3) purpose binding, 4) the right to correct or amend information, and 5) quality of recordkeeping. These principles (together with the OECD Guidelines on privacy and personal data) formed the basis for personal data protection law. For the purpose of this article it is important to note that while personal data protection law also applies to public entities, the application of surveillance technologies for law enforcement purposes is for the most part governed by the laws of criminal procedure.

We may conclude that privacy as a ‘physical state’ (i.e. the absence of information about, or interaction with an individual) receded as our society

---

9 Olmstead v. the United States, 277 U.S. 438, 478 (1928).
became more and more digitised and that data protection rules were put in place to remedy this situation.

2010-2020 Ubiquitous computing
We are currently in the early stages of the third phase of computer development, which Weiser and Brown have named the phase of ‘ubiquitous computing’. In the first phase of computing (the mainframe era), when computing power was still scarce, many people shared one computer (the mainframe). In the second phase (the PC era), computing power became so cheap, that (almost) every person could own a computer. Now, after a transition phase in which computers became connected through the internet, computing power is so cheap that countless computers can be embedded in our physical world. More or less, this is a reversal of the first phase: instead of many people sharing a computer, many computers ‘share’ a single person.

The era of ubiquitous computing will greatly benefit mankind: our environment will be able to respond intelligently to our presence in the physical space. This ‘ambient intelligence’ will make our lives easier, more efficient and safer. As Weiser pointed out in his seminal article on ubiquitous computing, computing will recede to the background of our lives, ushering in an age of calm technology where computers aid and support us in an unobtrusive manner.

While ubiquitous computing has the potential to greatly enhance our lives, it also brings with it significant risks for the (informational) privacy of individuals. In order to function properly and aid persons in their daily lives, the ambient intelligent environment has to process huge amounts of (personal) data. These data are not only gathered and accessed in ‘cyberspace’, they are for the most part gathered in the physical world and have their effects there as well, leading to potential breaches of informational privacy that are currently not possible. This threat is compounded by the fact that the design philosophy of ubiquitous computing is to make computing unobtrusive and invisible. So, while the possibilities for gathering personal data will be enhanced, transparency will greatly diminish.

2020-2040 The rise of NBIC technologies
According to Kurzweil, the convergence of nanotechnology, biotechnology, information technology (in particular artificial intelligence), and insights from the cognitive sciences will ultimately bring about Singularity. But even before we reach the Singularity point, NBIC technologies, by themselves or in convergence, will significantly impact society and our notions of privacy within that society.

12 Weiser & Brown 1996.
15 Teeuw & Vedder 2008.
Nanotechnology for instance, will allow for the creation of extremely small surveillance equipment, which will be (almost) impossible to perceive with the naked eye. Apart from the size of surveillance equipment, advances in nanotechnology and information technology will vastly reduce the price of surveillance equipment in general, allowing for their implementation in every corner of our physical world.

Artificial intelligence will also have a great impact on privacy, in particular in relation to surveillance. Currently, the sheer amount of data gathered by surveillance equipment makes it nigh impossible to process effectively. The volume of data thus becomes too great to yield information and knowledge, a problem known as ‘information overload’. Artificial intelligence promises to solve the problem of information overload. Moreover, advances in the area of data-mining will enable computers to ‘predict’ behaviour to an increasing extent. Furthermore, artificial intelligence will enable machines to identify objects, people and situations. Already facial recognition software is used to identify people. In the (near) future not only the accuracy of this software will increase, but also its capabilities will expand. For instance, intelligent cameras could scan a person’s face and recognise the emotional state of that person (happy, angry, frightened). This information can then be used to make predictions about the behaviour of the person (is this person about to commit a violent act? Is this person behaving suspiciously?). Currently, human operators perform this task, but unlike their computer counterparts, humans cannot perform their tasks indefinitely. Artificial intelligence can thus overcome the basic limitations of human surveillance operators: 1) the inability to process vast amounts of data, and 2) limited attention span.

Another way in which NBIC technologies may threaten privacy is through their destructive capabilities. NBIC technologies have the potential to place the capabilities for mass destruction in the hands of individuals. Examples of this include nano-pathogens and destructive self-replicating nanobots. In turn, the proliferation of this new breed of weapons of mass destruction (or the threat of their proliferation) will prompt the need for increased surveillance.

Nearing the Singularity
Ultimately, the convergence of NBIC technologies will bring us closer and closer to Singularity. The implications of (near)-Singularity technology applications for privacy, identity and personal autonomy will be so profound that our current ‘pre-Singularity’ privacy issues seem petty by comparison. In my opinion, two related technological developments that will have an immense impact on privacy are 1) brain-machine interfaces and 2) the reverse engineering of the brain.

The first technological development that will severely impact privacy is direct brain-machine interfacing. In order to interact more efficiently and
effectively with the technology that will surround us, we will increasingly use direct brain-machine interfaces. While this allows us to interact directly with machines in an intuitive manner (and on an almost subconscious level), it will also open up a link between the outside world and our brain. This means that our bodies and brain will no longer be a bastion of privacy and personal identity, but may become ‘visible’ for others. This will not only challenge notions of ‘public’ and ‘private’ but even challenge notions of ‘individual’ and ‘collective’. So, while direct brain-machine interfaces will make us vastly more efficient and effective as human beings, they also bring with them significant new threats. Since brain-machine interfaces will work both ways, it might become possible to examine, visualise, and record a person’s thoughts.

The second technological development will severely impact privacy is the ‘reverse engineering’ of the brain. Our knowledge on the human brain and the way in which it works continues to grow every day. Since the cognitive sciences are becoming increasingly adept at reverse engineering the human brain, it will become possible in the future – to some extent – to predict a person’s behaviour. Already experiments are under way aimed at ‘sensing’ people’s thoughts and feelings and it is likely that this trend will continue.17

**What is the problem?**

Currently, physical boundaries (walls, doors, the mind) and the limits of the human brain (e.g. fading memories, limited attention span) still provide us with some measure of privacy. However, these ‘physical’ boundaries will disappear once ubiquitous computing and NBIC technologies develop further. As mentioned before, even the mind may ultimately fail as a bastion of privacy. Therefore, privacy as a ‘physical state’ or ‘physical reality’ will disappear within the next twenty years.18

From the above we have seen that once privacy as a physical state disappears; regulations are put in place to recreate artificially the lost measure of privacy. So what is most interesting to note about the end of privacy is that the (possible) destruction of privacy in a certain instance creates the need for a right to privacy in that very same instance. Thus, while privacy as a physical property is disappearing, the need for a strong right to privacy is growing.

17 For instance, brainwave fingerprinting is a controversial forensic technology that can determine whether a person is lying on the basis of brainwave readings. In 2001, results from a brainwave fingerprint were admitted as evidence in a criminal case in the United States (Harrington v. State, Case No. PCCV 073247. Iowa District Court for Pottawattamie County, March 5, 2001).

18 See also: Schermer 2007.
In the following section, I shall describe why the right to privacy is so important, in particular in the age of ubiquitous computing and the following age of converging NBIC technologies. I argue that (the right to) privacy protects individuals and groups against the dangers of information asymmetry, paternalism, mistakes, and risk justice.

Information asymmetries
An important role of privacy (or a right to privacy) is preventing information asymmetries. When one party has intimate knowledge about another party as a result of surveillance, and the other party lacks a similar form of knowledge, the resulting information asymmetry creates a disturbance in the balance of power between these parties. The essence of surveillance is strengthening one’s information position and as such surveillance creates information asymmetries almost by definition. Privacy has always acted as a natural barrier against information asymmetries, and in the absence of privacy, the right to privacy.

Paternalism
As technology becomes more effective at identifying and classifying human behaviour, the ability to influence our behaviour will grow. This in turn might lead to paternalism on the part of those in power. This is compounded by the fact that ubiquitous computing and NBIC technologies will enable us to influence the physical world in real time. An example of this can already be seen in England where CCTV operators not only observe the physical space, but also actively influence it. When someone displays behaviour that is considered inappropriate (littering, loitering, vandalism), CCTV operators call out to the person in question over a loudspeaker in an effort to alter their behaviour.

Mistakes
An issue with surveillance in general is that of false positives and false negatives. Since surveillance technology is not infallible (nor is it likely ever to become infallible), surveillance systems will also point out people who are in fact not criminals or terrorists at all (so-called false positives). The other problem is false negatives. Since most of the information on crime and terrorism that will guide surveillance is based on previous experiences and behaviour, new forms of deviant behaviour may escape attention. Since criminals and terrorists also innovate, they will employ new methods and use new attack vectors that are not detected by surveillance systems. False positives and false negatives may undermine the trust in surveillance systems, reducing the legitimacy of their use.

Risk Justice
The desire for risk-management and security in society has had a significant influence on the development of criminal law in recent years. It could be
said that we are moving towards a system of ‘risk justice’. In such a system, the focus is not on solving crime and the legal punishment of criminal offences, but rather on the prevention of criminal offences and the reduction of risk. In both substantive criminal law and the law of criminal procedure we can clearly discern the development of risk justice. The scope of criminal liability for instance, has been greatly expanded over the past years, most notably in the area of terrorism. The increased criminal liability creates a ‘gray area’ in the law between merely thinking about a criminal act and actually committing one, where sweeping investigative powers and surveillance may be used nonetheless. One could argue that the change this has brought in our criminal justice system is that it is no longer just the actual criminal act that is punishable, but also the thought of a criminal has become punishable. It is clear that this situation can lead to mistakes and arbitrary decisions by law enforcement agencies that could threaten the privacy and liberty of individuals.

There is an interaction between the expansion of criminal liability (substantive criminal law), the use of investigative powers (criminal procedure) and the development of technologies that can sense and predict behaviour (surveillance technology). As these technologies become more advanced and the pressure to use them higher (for instance because individuals will have the power of mass destruction through weaponised NBIC technologies), substantive criminal law and the law of criminal procedure will open up possibilities for their use. In turn, this will lead to new efforts to develop advanced surveillance technologies.

Ultimately, it is not unthinkable that in a near Singularity society, the government could use the power of human-brain interfaces and reverse engineering of the brain to detect thoughts that are considered dangerous for the well-being of society. With brain-machine interfacing and increasing knowledge of the human brain, the idea of the persecution ‘thought crimes’ might thus become a reality.

The right to privacy

We may conclude that privacy as a ‘physical reality’ is quickly becoming a thing of the past. Privacy as a physical barrier to the observing gaze of others will no longer be a reality in a near-Singularity society. One could therefore argue that since the protection of privacy is a lost cause, we should abandon any hopes of retaining it all together. Scott Neally, CEO of Sun Microsystems, already stated in 1999 that: “you have zero privacy anyway, get over it”.

But from the above we may also conclude that the erosion of privacy in near-Singularity societies brings with it such significant risks for individuals, that we will continue to need a right to privacy. So, we have to rely on...
Deel V – Privacy

the law (i.e. the right to privacy) for the protection of the interests (most nor-
ably individual liberty) hitherto protected by privacy in a physical sense.
However, unlike physical barriers, rights, especially individual rights, can
be revoked for the good of the community as a whole. In particular the
destructive capabilities of NBIC technologies might trigger the need for
greater, more infringing investigative powers. The problem of risk justice
described in the previous paragraph seems to indicate that this is indeed the
trend for the coming years.

The prospect of destructive NBIC technologies, the possibility of perva-
sive surveillance, the resulting disappearance of privacy, and the prospect of
risk justice will severely challenge the legitimacy of our law systems. It is
therefore important to find ways to strengthen the right to privacy and the
interests it aims to protect.

The way forward

From the above we may conclude that while privacy as a physical barrier
will disappear in the future, the right to privacy will become increasingly
important. However, the fact that privacy will no longer be part of our phys-
ical reality but merely a ‘legal concept’ means that the right needs to be
strengthened. Below I shall describe some measures aimed at strengthening
and supporting the right to privacy.

Privacy by design

First of all, it is important to maintain whatever ‘physical privacy’ we can.
To this end we must turn to ‘privacy by design’. Privacy by design is a
design philosophy whereby privacy rules are incorporated in the design of
information system. By ‘hardwiring’ privacy rules into technology, unnec-
essary breaches of privacy are prevented. Means of reducing the availability
of personal data through technology include anonimisation, authentication,
and selective disclosure. Privacy by design is more effective than legal pro-
tection in itself, since rules can be broken or changed, whilst the design of
an information system forces users to comply with the rules set forth in the
design.

However, even when systems are designed with the principles of priva-
cy by design in mind, it will be nigh impossible to maintain privacy as a
physical barrier. In my opinion we must therefore also look towards other
mechanisms for ensuring privacy.

Transparency and reciprocity (by design)

We have established that one of the main problems with surveillance is infor-
mation asymmetry, a fact that will be compounded by the nature of ubiqui-
tous computing in the next years and by NBIC technologies thereafter.
Authors like Bailey and Brin have looked towards (reciprocal) transparency
Privacy and Singularity: little ground for optimism?

as a means to negate information asymmetries. The idea of reciprocal transparency and the related notion of sousveillance, are based around the premise that surveillance power should be equally distributed.

For the next twenty years or so, the challenge is to remedy the ‘black box’ nature of ubiquitous computing. A major part of the design philosophy for ubiquitous computing systems is that they should not burden the user. Ideally, their use should be unobtrusive and intuitive. But this design philosophy also makes the information systems less transparent. An approach is therefore necessary that entails that the data subject is properly informed about acts of data processing in order to keep a form of reciprocity between the data subject and the company or institution using his data. Where possible such an approach should be built into the technology.

The need for transparency will become even greater when nanotechnology will allow for truly pervasive surveillance. Without strict rules on the application of nano-surveillance, proper purpose specification and the ability for users to scan their surroundings for surreptitious nano-surveillance, the balance of power will be severely upset.

But transparency is not only important for the protection of the individual, it is also necessary to foster trust in surveillance. Evidence suggests that when individuals perceive that others are behaving cooperatively, they are moved by honour, altruism, and will be inclined to contribute to public goods even without the inducement of material incentives. When, in contrast, they perceive that others are shirking or otherwise taking advantage of them, individuals are moved by resentment. In that circumstance, they will withhold beneficial forms of cooperation. We may infer from this that when surveillance infrastructures are no longer perceived to be beneficial to those under surveillance, or their operation is no longer transparent, they will elicit negative responses from groups and individuals. This could lead to the evasion of surveillance or possibly even the sabotage of surveillance infrastructures.

User empowerment
Currently individuals are for the most part unaware of the fact that personal data about them is being gathered through the various technological infrastructures that surround them (e.g. mobile phones, internet and CCTV). Furthermore, they have little to no influence on these technological infrastructures and the data they process. This situation will likely worsen in the future, since ubiquitous computing and NBIC technologies will be even less visible and tangible than current technology.

If users are to retain their right to privacy in the future, they must be given the means to exercise this right. This means that users must have a right to know whether surveillance infrastructures are present, get an idea

---

21 Kahan 2009.
who is using them, and what the purpose of the surveillance system is. While current data protection law and associated laws aimed at protecting privacy already grant these rights to individuals, the problem is that individuals do not have the power to actually effectuate these rights. Therefore, user empowerment is of the utmost importance.

First of all users need to have the means to detect surveillance systems. To this end they will need (automatic) detection tools (e.g. RFID detectors, software privacy agents, privacy coaches and nano-surveillance sniffers). By providing these tools we can enhance the transparency of surveillance and avoid unwanted and invisible surveillance. Second, users must also get some manner of agency. In other words, they must have the ability to influence the use of their personal data and shield themselves from unwanted observation.

What must be noted about this approach though, is that while workable in the context of business-to-consumer or consumer-to-consumer privacy issues, it is not well suited for use in a surveillance context. The reason for this is that when it comes to surveillance of suspects, oftentimes you do not actually want the subject to be aware of the surveillance. Furthermore, you do not want to give tools to avoid or counteract surveillance to potential criminals and terrorists. As such, user empowerment has its limitations.

**Accountability**

Whereas individual user empowerment is difficult in the context of state surveillance, it is possible to restore the balance between the surveillors and the surveilled through proper accountability. Therefore, we should place more emphasis on the accountability of surveillance. We must ensure that proper checks and balances, judicial oversight, and regular reviews of surveillance practices are in place. Furthermore, sunset clauses should be introduced for particularly invasive surveillance technologies and investigative powers in order to ensure that their application cannot go on indefinitely without proper consideration. Not only are these measures necessary to ensure the legitimacy of surveillance practices, they also foster trust in their application.

**Privacy as a collective interest**

Currently privacy is conceptualised as an individual right. However, the interests that privacy aims to protect are actually also collective interests (e.g. trust, autonomy, social cohesion and equal treatment). Thus, positioning privacy as an individual right may actually be counterproductive, because the secrecy normally associated with privacy will reinforce notions of the collective versus the individual. By positioning privacy as a prerequisite for the development of a stable, democratic and free society, discussions that position an individual’s right to privacy versus the security of society as a whole can be avoided.

---

Emphasis on identity and autonomy

Personally, I feel that if the predictions of Vinge, Kurzweil, and other Singulatarians are accurate, we need a far stronger emphasis on identity and autonomy in the discourse on privacy and data protection. The possible near-Singularity privacy issues set forth in this article are so fundamental for the autonomy of the individual, that an accompanying vocabulary must be used.

The concept of privacy and it conceptualisation as a right has been subject to inflation over time. While human rights such as the freedom of speech or the freedom of religion are (almost) unchallenged in the political debate, the right to privacy, which in my opinion is equally important and a prerequisite for many other fundamental rights, is regularly challenged. This can in large parts be attributed to the association of privacy with secrecy and hiding. So, instead of merely repositioning privacy as a collective interest, we need a new vocabulary for future privacy issues with a strong emphasis on the importance of personal identity and autonomy. For instance, instead of arguing about the privacy aspects of brain-machine interfaces we should push for a ban on state intervention in the thoughts of individuals. This would block the use of brain-machine interfaces for surveillance purposes and frame the discussion on the more fundamental level of personal autonomy.

Conclusion

The technological Singularity as described by Vinge and Kurzweil, if it ever occurs, will have such a profound impact on mankind that we cannot begin to describe the ethical and societal consequences it will entail. The aim of this article has therefore not been to describe the legal issues that arise after the Singularity, but rather describe those likely to emerge prior to Singularity. When we take the ‘soft take off’ scenario and look at the technological developments that will culminate in Singularity, we see that these technologies alone and in convergence, will have a significant impact on individuals and society as a whole.

In this article, I focussed on the possible consequences of near-Singularity technology for privacy. In my opinion privacy as a physical barrier against the observing gaze of others will steadily disappear over time as new, more advanced surveillance tools become available. So, to answer the first part of the problem statement would be that the effect of near-Singularity technologies on privacy will be no less than the disappearance of privacy as a meaningful physical barrier against the observing gaze.

23 Blok 2002.
24 A Dutch chief of police even went so far as to say that privacy is ‘the hiding place of evil’.
The second part of the problem statement is much more difficult to answer. We can strengthen the right to privacy through measures like privacy by design, transparency and user empowerment, but this will be insufficient and sometimes even impossible in the context of state surveillance.

In my opinion a significant step in safeguarding (the right to) privacy in the future, particularly in the context of surveillance, is acknowledging its importance. Privacy is a prerequisite for our personal autonomy and human dignity, but in the context of surveillance is seen mainly as an obstacle for effective law enforcement. Such an attitude, while understandable, is dangerous. In my opinion we need to stop viewing privacy as an individual right (associated with secrecy), but must also consider it a collective interest, necessary for the well-being of our society. Furthermore, since future technologies may impact privacy at such a fundamental level (i.e. at the level of our personal thoughts) we need to frame the discussion at this fundamental level. This means more emphasis on the risks of surveillance for personal identity and autonomy.

We may conclude that the power of near-Singularity technologies is significant and that there will be considerable pressure to use them. Furthermore we may conclude that there seems to be little attention for the possible negative effects of these technologies for our privacy. If we fail to address these negative effects, Professor Schmidt was right in saying that there is little ground for optimism.

REFERENCES

Aarts, Harwig & Schuurmans 2002

Bailey 2004

Blok 2002

Brin 1999

Kahan 2009

Kurzweil 1990

Kurzweil 1999

Kurzweil 2005
Privacy and Singularity: little ground for optimism?

Moerings 2006

Schermer 2007

Schmidt 2009
Schmidt (2009), E-justice: No Ground for Optimism, Leiden University.

Solove 2008

Teeuw & Vedder 2008

Vinge 1993

Warren & Brandeis 1890

Weiser 1991

Weiser & Brown 1996

Westin 1984