amsterdamlawforum
VU University Amsterdam

SURVEILLANCE AND PRIVACY IN THE UBIQUITOUS NETWORK SOCIETY

Mr. dr. Bart W. Schermer[*]

Introduction

In the course of just thirty 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 led to significant changes in the way we structure our lives and our society. But as digital technology progresses we will likely witness an even more profound shift.

According to Wooldridge, the history of computing has been marked by five important and continuing trends: *ubiquity*, *interconnection*, *intelligence*, *delegation,* and *human-orientation*.[1] The first trend is a result of the reduction in the cost of computing. The low cost of computing power allows for its incorporation into a host of different (everyday) devices making computing progressively more ubiquitous.[2] The second trend is towards the interconnection of computer systems into large networked and distributed systems such as the internet. The third trend is towards the creation of progressively intelligent computer systems able to perform increasingly difficult and complex tasks. The fourth trend is towards the delegation of control from the human actor to the computer. The fifth trend is towards the creation of computer interfaces that more closely reflect the ways in which humans interact with their surroundings. Together, these trends will bring about a 'Ubiquitous Network Society'; a society in which every aspect of our daily lives is networked and connected.[3]

Ubiquitous computing is dependent on the processing of data for its effectiveness. As such, vast amounts of data will be processed in the Ubiquitous Networks Society. These data include location data, personal data, object related data, and transactional data. But while computing power will become ubiquitous, and the processing of data will become pervasive, the visibility of data processing will decrease. As Mark Weiser put it: "The

---

[*] *Bart Schermer is assistant professor at the University of Leiden (faculty of law, eLaw@Leiden), fellow at the E. M. Meijers Institute for legal studies, and partner at consultancy firm Considerati.* *This publication was made possible by the Secure Haven Project.*

[1] M. Wooldridge, *An Introduction to Multi-agent Systems*, West Sussex: John Wiley & Sons Ltd., 2002.

[2] M. Langheinrich, 'Privacy by Design – Principles of Privacy Aware Ubiquitous Systems', *Proceedings of Ubicomp 2001*, Springer-Verlag LNCS 2201, 2001, pp. 273-291.

[3] T. Murakami, 'Establishing the Ubiquitous Network Society in Japan: from eJapan to uJapan', *NRI Research Papers no. 66,* July 2003.

most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."[4]

Pervasive computing and information processing coupled with decreasing transparency due to diminishing visibility will present serious challenges to our society. Risks associated with data processing are: breaches of confidentiality, information asymmetries and misinterpretation of available data.

Currently, invoking the right to privacy mitigates risks associated with the processing of personal data. The right to privacy ensures that we can shield ourselves, and our personal data, from the prying eyes of others. However, in a future of ubiquitous computing, where pervasive information processing is the norm, it will become harder to maintain (informational) privacy. Moreover, the distinction between the public and the private sphere will become increasingly blurred as a result of ubiquitous computing. This places our current notion of privacy under pressure. It is therefore necessary to examine how privacy will evolve, and ascertain whether it can provide adequate protection against excessive surveillance.

In this article I will describe 1) how developments in IT will enable new surveillance applications, 2) what possible risks these new surveillance applications entail, 3) how the notion of privacy will be influenced by these technologies, and 4) how we can protect ourselves in the future.

I. Technology

The convergence of trends like ubiquity, interconnection, intelligence, delegation, and human-orientation will ultimately bring about the Ubiquitous Network Society. Key technological drivers for the development of the Ubiquitous Network Society are automatic identification and data capturing, mobile networking and artificial intelligence.

I.1. Automatic Identification and Data Capturing (AIDC)

A central element of the Ubiquitous Network Society is that objects in the physical world will be able to communicate with us and with each other. To this end they need to have a unique identity (e.g. an IP-address), sensor capabilities to sense objects or persons in the physical world, and the ability to transmit information. By employing technologies such as Radio Frequency Identification (RFID), Near Field Communication (NFC), 2D matrix codes and different types of sensors (e.g. motion sensors, heat sensor and cameras), we can create 'an internet of things'.

I.2. Mobile Networking

While AIDC technologies provide 'last (centi)meter connectivity', powerful third and fourth generation mobile networks provide the connection

[4] M. Weiser, The Computer for the 21st Century*, in: Scientific American Special Issue on Communications, Computers, and Networks*, September 1991.

between people and the internet. Mobile internet is rapidly expanding and enables us to connect with vast repositories of information from any location. By adding GPS and other localisation tools to mobile equipment, location based services and geo-location become possible. Currently, these features are packed within so-called smart-phones. In the future, Heads-Up Displays in glasses or even in contact lenses will become the norm.

I.3. Artificial Intelligence

Artificial intelligence technologies enable computers to recognise patterns (such as faces) and make sense of vast amounts of data that need to be processed in order to respond effectively and efficiently to situations in the physical world. Through artificial intelligence, our physical world can become an intelligent environment that can react to our wishes, wants, and needs.[5]

II. The Transformation of the Public Domain

Currently, the public domain is an area where, apart from closed circuit television (CCTV) and the location data of mobile phones, little data is recorded. The digital world is thus, for the most part, separated from the physical world. But through the integration and convergence of the above-mentioned technologies, the digital world and the physical world will become increasingly intertwined, significantly altering our ideas about the public domain.

For the topic discussed in this paper (i.e., the future of privacy and the public domain in relation to surveillance), the most relevant applications of surveillance technology in the Ubiquitous Network Society are 'mirror worlds' and 'augmented reality'.

II.1. Mirror Worlds

Mirror worlds are information-enhanced virtual models or 'reflections' of the physical world. Their construction involves sophisticated virtual mapping, modelling and annotation tools, geospatial and other sensors, and location-aware technologies.[6] Google Earth is a good example of a mirror world application. Mirror worlds can be based on recorded information (e.g. photos, historical data, maps of buildings), but as we move towards the Ubiquitous Network Society, we will move towards mirror worlds that operate in real-time.

Mirror worlds enable us to get a clearer picture of what is happening in the physical world. Currently we mainly use sensor technologies (predominantly CCTV) to establish what is going on at a certain place, but these sensor data are not combined with other sources of information such as geographical data, historical data, newsfeeds, data from UAVs (unmanned aerial vehicles),

---

[5] E. Aarts, S. Marzano, *The new everyday view on ambient intelligence*, Rotterdam: 010 Publishers, 2003.

[6] E. Castranova *et al.*, *Metaverse Roadmap, Pathways to the 3D Web*, Acceleration Studies Foundation 2007, p. 9.

information from onsite actors *et cetera*. By combining various information feeds, situational awareness can be enhanced, thereby making the decision making process more effective and efficient.

Situational awareness is vital for effectively implementing command-control structures. It is therefore not surprising that the idea of ubiquitous networking and integration of data sources features prominently in modern military doctrine (the doctrine of network-centric warfare). The police are also leveraging the advantages of information technology. This has led to the notion of 'intelligence led policing', whereby crime control focuses upon the identification, analysis and management of persisting and developing problems or risks.[7] Intelligence led policing allows for the more efficient and effective application of limited police resources. By using pre-recorded and analysed data, as well as real-time information, police tasks can be executed more efficiently.

Apart from heightening situational awareness, mirror worlds can also be used to influence the public domain in real-time. A current example is traffic management. Operators can dynamically display the maximum speed on matrix signs over the roads depending on the current traffic situation. Heightened situational awareness, coupled with networked objects and infrastructures in the physical world (e.g. gates, roadblocks, screens, microphones) will allow for more direct control over our physical world. For instance, when a demonstration threatens to turn violent, operators could 'change' the architecture of a public place by closing off roads or setting up choke points in order to control the size of the crowd and deny access to certain areas. Moreover, they could use TV screens and microphones to address the crowd.

II.2. Augmented Reality

Mirror worlds provide a representation of the physical world that exists as a separate entity. In other words, mirror worlds are models, representations and copies that exist solely in cyberspace. While they can be used as tools to make sense of the physical world, and even directly influence it, they are separated from everyday reality. This is set to change through augmented reality. In augmented reality, technology enhances the external physical world for the individual through the use of location-aware systems and interfaces that process and layer networked information on top of our everyday perception of the world.[8] As such, augmented reality integrates the digital and the physical world into one coherent reality. While mirror worlds can give a high level overview (i.e., strategic and operational) used for command-and-control purposes, augmented reality can provide rich information for units 'on the ground'.

---

[7] W. De Lint, 'Intelligence in Policing and Security: Reflections on Scholarship', *Policing & Society*, Vol. 16 no. 1, March 2006, pp. 1-6.

[8] Castranova, 2007, *supra* note 6, p. 12.

A good example of a possible future augmented reality application is given in the novel *Halting State* by Charles Stross. In this novel, Stross describes how police officers, wearing special glasses, have a layer of additional information projected on top of the physical world in order to help them with their police work. This hybrid reality, which mixes real world images with information from the digital world, is called 'CopSpace':

"…CopSpace sheds some light on matters, of course. Blink and it descends in its full glory. Here's the spiralling red diamond of a couple of ASBO cases on the footpath (orange jackets, blue probation service tags saying they're collecting litter.) There's the green tree of signs sprouting over the doorway of number thirty-nine, each tag naming the legal tenants of a different flat. Get your dispatcher to drop you a ticket, and the signs open up to give you their full police and social service case files, where applicable... …This is the twenty-first century, and all the terabytes of CopSpace have exploded out of the dusty manila files and into the real world..."[9]

Through augmented reality, users can gain access to relevant information about objects, locations and even individuals in real-time, aiding them in their decision making process.[10]

III. Consequences and Risks

Mirror worlds and augmented reality will change the way in which we view the public domain. Moreover, the use of these technologies for surveillance purposes can significantly impact individuals in the public domain. In this section/chapter I shall describe some possible risks associated with surveillance in the Ubiquitous Network Society.

III.1. The (Super)Panopticon

In 1791, social reformer and philosopher Jeremy Bentham introduced a new type of penitentiary design he called the 'Panopticon'.[11] The aim of this revolutionary prison design was to keep the inmates under close and continuous scrutiny. The prisoners were not allowed any private space and were given the impression that they could be watched at all times. Hence, Bentham named his prison design the 'Panopticon', Greek for 'all-seeing place'. The essence of surveillance according to Foucault is the accumulation of information and the direct supervision of subordinates.[12] The panoptic concept is therefore associated with current electronic surveillance practices. However, the use of electronic surveillance has moved beyond the confines of a single prison, and is prevalent all around us. Therefore, Poster has described surveillance in our society as being 'superpanoptic'.[13] The Panopticon brings with it two specific risks that threaten the autonomy of

---

[9] C. Stross, *Halting State*, New York: Penguin Books 2007, p. 82.
[10] For a current example of augmented reality see: http://layar.com/
[11] J. Bentham, *Jeremy Bentham: Collected Works* (ed. Bowrning, J.), London, 1843.
[12] D. Lyon, *The Electronic Eye, the Rise of Surveillance Society*, Minneapolis: University of Minnesota Press 1994, p. 66.
[13] M. Poster, *The Mode of Information*, Cambridge: Polity Press 1990.

the individual: direct and indirect discipline.

First, surveillance facilitates direct discipline by giving those employing it more power over the subjects being surveilled. In a Ubiquitous Network Society this risk is even greater. Not only because there is more information available, but also because surveillance will increasingly be in real-time. Currently, surveillance information is, for the most part, used *ex-post*. However, this will change with the rise of the Ubiquitous Network Society. Given the fact that the digital world and the physical world will be closely intertwined, surveillance operators will even have the ability to trigger events and actions from a distance as mentioned above. This development will change surveillance from an 'architecture of observation' to an 'architecture of control', which will negatively impact the autonomy of individuals and groups who move through the public domain to a far greater extent than currently possible.

Second, there is the risk of indirect discipline. Foucault described the Panopticon as a "subtle, calculated technology of subjection".[14] For him the Panopticon was a means to "induce in the inmate a state of conscious and permanent visibility that ensures the automatic functioning of power".[15] The actual exercise of power is no longer necessary, since the subjects are aware that they are constantly being watched and will alter their behaviour accordingly. So instead of external discipline, the Panopticon establishes a situation where the inmates actually discipline themselves. The same logic could apply to surveillance in society.

Whether permanent surveillance in the public domain will have a self-disciplining effect on citizens remains unclear. Currently, with the use of CCTV for instance, people seem to experience little panoptic feelings. This can best be explained by two factors. First, for the most part citizens feel that the observing gaze of the CCTV cameras is benevolent. People assume that it adds to their security and that they as law-abiding citizens have nothing to hide. Second, people do not yet experience the use of CCTV as a form of permanent visibility. But in the Ubiquitous Network Society the possibility that some form of permanent visibility is established is much greater than in our current society. Also, the disciplining effects of surveillance will be much more evident when actions can be taken in real-time by the surveillance operators. Raised awareness of direct discipline might in turn lead to self-disciplining or 'indirect-discipline'.

III.2. Lack of Transparency

One of the characteristics of the Ubiquitous Network Society is that 'computing will move to the background of our lives'. In other words, it will become less obvious how, why, when and where personal data is being

[14] M. Foucault, *Discipline and Punish, the Birth of the Prison*, New York: Vintage Books 1975, p. 201.
[15] Ibid.

processed. Furthermore, it will become less clear who has access to the data being processed.

First of all, transparency is hampered by the technology itself. In the Ubiquitous Network Society information gathering will for the most part be unobtrusive. In other words, it will not always be clear for data subjects that personal data is being processed. This is part and parcel of the ubiquitous computing design philosophy: interaction with information systems should be intuitive, and users should not be burdened. Unfortunately, this same design philosophy also entails that for most users, pervasive computing systems are 'black boxes'. While from a design and computing perspective these are sometimes preferable qualities (they may decrease intrusiveness of ICT), from a legal perspective these design principles can be less desirable, since they shift away control (and thus power) from the individual.[16]

A second problem with the transparency of surveillance in the Ubiquitous Network Society is the multitude of actors involved. While the (super)panoptic model is highly relevant as a metaphor for the development of the surveillance society, it does not accurately reflect the way in which surveillance will be conducted in the Ubiquitous Network Society. The sensor- and data feeds will fuel mirror worlds, and augmented reality will not exclusively belong to public sector actors. On the contrary, most of the data will belong to private actors, such as companies and individuals. As such, there is no single controlling entity (i.e. the state) in the Ubiquitous Network Society, as implied in superpanoptic theory. The idea that surveillance is not exclusively conducted by the state has led Haggerty and Ericson to come up with the notion of the 'surveillant assemblage'.[17] An assemblage is not a discretely bounded, structured, and stable whole, but is made up of a multitude of interrelated parts. In the surveillant assemblage there is no single entity in control of all these systems, but rather control is distributed throughout a host of different actors in society. As such, it will become less clear who is in control of the data and who has access to it, thus creating a lack of transparency.

The fact that surveillance infrastructures will not exclusively belong to the state, does not imply that the state will not have access to private surveillance infrastructures and even personal data feeds. Surveillance is driven by the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole. It is likely that the integration and convergence of technologies will lead previously discrete surveillance systems to become increasingly interlocked.[18] In this way the state can 'tap' into the

---

[16] By a black box we mean a system of which the workings are unknown to outsiders. In other words, it is unclear how input is being processed and how output is created.

[17] K. D. Haggerty, R. V. Ericson, (2000). 'The Surveillant Assemblage', *The British Journal of Sociology*, Vol. 51 Issue 4, 605, December 2000, pp. 605-622.

[18] M. Innes, *Understanding Social Control: Deviance, Crime and Social Order*, Berkshire: Open University Press, 2003, p. 126.

private sector surveillance apparatus and obtain additional surveillance data. As such public sector and private sector surveillance will become closely integrated.[19] So while the possibilities and effectiveness of state surveillance will be greater, there will be less control and oversight.

III.3. Digital Discrimination

While mirror worlds, augmented reality, and other surveillance tools can aid in applying scarce police resources more effectively, they also create the risk of excessive trust in the system, which in turn might lead to 'digital discrimination'.

Since humans are unable to process all the different data feeds that the ubiquitous network provides at the same time, filtering mechanisms will be used that present the data to humans in a structured and comprehensible way. However, this also means that information will be displayed in a compressed way. In particular with augmented reality, police officers will likely use the limited information on individuals presented to them as their lead for follow-up actions (e.g. pulling people over, searches and seizure). While this can be beneficial, it also creates the risk that the police officers will rely too much on the system and its underlying assumptions, possibly bypassing their own personal insights, experience and other factors. By ignoring important contextual information not included in the 'digital file' of a person or not relying on their own insights, police officers could overlook vital information, or become (more) biased in their actions against certain individuals or groups. For instance, ethnic registration and racial profiling could lead to discrimination of minorities. Another example could be ex-criminals who would literally be followed around by their criminal record, leading to increased and possibly unwarranted police attention.

III.4. False Positives and False Negatives

An issue with surveillance in general is that of false positives and false negatives, and this is also true for surveillance in the Ubiquitous Network Society. Since surveillance technology is not infallible, it is likely that surveillance systems will also point at people who are in fact not criminals or terrorists at all (false negatives). Even with a 99% accuracy rate, this will mean that in public places, where there are a lot of people, the number of false positives will be considerable. 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 innovate too, they will employ new methods and use new attack vectors that are not yet detectable by surveillance systems.

In summary we can state that in the future the power of surveillance and its effect on life in the public domain will be greater, while the transparency of surveillance will decrease. This will lead to information asymmetries between the surveyors and those being surveilled. Without proper oversight and

[19] D. Lyon, *Surveillance after September 11*, Cambridge: Polity Press 2003, p. 105.

checks and balances, surveillance may pose an increased threat to personal autonomy. Up until now, the right to privacy is used to negate any information asymmetries, however, it is unclear whether this will be sufficient in the future.

IV. Privacy

The need for privacy is probably as old as mankind itself, and virtually all societies, both primitive and modern, have techniques for setting distances and avoiding contact in order to afford members of a measure of privacy.[20] Before the upcoming of modern technology, physical boundaries combined with rules, customs and taboo created a distinction between the 'public' and the 'private'. But as technology progressed, physical barriers became less effective in protecting privacy, making legal protection more important. Particularly the rise of information technology and electronic recordkeeping led to a changing notion of privacy. As the processing of personal data became commonplace, the focus of the privacy debate shifted from the protection of the 'classic' dimensions of privacy (body, home, and correspondence) to the protection of personal data.[21] The protection of personal data led to the notion of 'informational privacy'. Westin described informational privacy as:

"the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated."[22]

Privacy and the protection of personal data serve various purposes within our society. In the context of surveillance, privacy primarily serves as a limit to power and government intervention. Hiding information or denying access to it through the right to privacy can help avoid information asymmetries. Invoking the right to privacy thus protects the autonomy of groups and individuals. However, the Ubiquitous Network Society will bring new challenges to the concept of privacy that will make it difficult to maintain as a viable concept.

V. Challenges to the Concept of Privacy

Privacy has always been a concept in transition. New technologies in particular have led to changing ideas and notions of privacy. Now, as our society changes into a Ubiquitous Network Society, the concept of privacy is set to face yet another transformation. By definition, privacy is dependent on a distinction between what is public and what is private. The idea of (informational) privacy in the public domain is thus problematic. However, in the discourse on surveillance, (informational) privacy features prominently. When it comes to surveillance and privacy in public places there are two main questions that need to be answered: 1) who may be surveilled under

[20] J. Wagner DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology,* Ithaca: Cornell University Press 1997, p. 12.
[21] P. Blok, *Het Recht op Privacy*, Den Haag: Boom Juridische uitgevers 2002.
[22] A. F. Westin, *Privacy and Freedom*, New York: Atheneum Press 1967, p. 7.

what circumstances, and 2) how may data garnered from surveillance be used?

In surveillance discourse answers to these questions have mainly been sought in the doctrine of the reasonable expectation of privacy, personal data protection law and the law of criminal procedure. In my view, the doctrine of the reasonable expectation of privacy and the law of criminal procedure will not provide adequate protection in the Ubiquitous Network Society.

V.1. The Reasonable Expectation of Privacy

The reasonable expectation of privacy criterion limits the right to privacy to those instances where an individual indeed has a reasonable expectation of privacy. In other words, the individual must demonstrate the wish that his conduct remains private and society must acknowledge the fact that the individuals conduct is indeed private. The reasonable expectation of privacy thus entails two separate elements: (1) an objective element (how does the individual behave?), and (2) a subjective/normative element (what can the individual expect judging from his behaviour?). The answers to these separate questions determine whether there is a reasonable expectation of privacy. An indication that an individual may have a reasonable expectation of privacy can be that his behaviour takes place in an area that is considered 'private', examples being: at home, in his car, or in a fitting room.

But do individuals have the same subjective expectation of privacy when they are in the public domain (e.g. walking on the street, sitting in a park, waiting in line at city hall)? Probably not. And if they do, this expectation can shift once they become aware that opportunities for surveillance in the Ubiquitous Network Society are omnipresent. It is thus not surprising that the use of the reasonable expectation of privacy criterion has been widely criticised as useless, simply because reasonable expectations of privacy in a certain situation can disappear as soon as privacy is invaded on a routinely basis.[23] So the protection resulting from employing the reasonable expectation of privacy criterion is limited. Moreover, as 'privacy sensitive' technologies continue to develop, how will the reasonable expectation of privacy criterion hold up in the future?

V.2. The Law of Criminal Procedure

While data protection law provides us with clear requirements for the fair processing of personal data (e.g. notification, purpose binding, transparency), the law of criminal procedure (which governs surveillance for the most part) does not always set forth such requirements.[24] For instance, notification is

---

[23] P.E. Agre, (2001), 'Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places', *Whole Earth* 106 2001, pp. 74-77. See also A. Goodlad *et al.* (2009), 'Surveillance: Citizens and the State', *House of Lords Select Committee on the Constitution, 2nd Report of Session 2008–09*.

[24] See: 'Recommendation Concerning and Guidelines Governing the Protection of Privacy and the Transborder Flow of Personal Data', *Organisation for Economic Cooperation and Development (OECD)* 1980.

often impossible, because it would alert suspects that they are being watched. Furthermore, while personal data protection law to a large extent prohibits private sector actors from using personal data, the same rules do not necessarily apply to surveillance by public sector actors. Once data enters the public sphere, it is for the most part considered 'available' for surveillance purposes, since data subjects do not have a reasonable expectation of privacy with regard to data they willingly place in the public sphere. For instance, information published by users on their social networking site can be used as evidence in a criminal procedure. The same logic could apply to personal data processed in a fully networked public domain.

VI. Safeguarding Privacy and Autonomy

From the above we may conclude that privacy will become increasingly hard to conceptualise and apply as a workable concept in the context of surveillance and the Ubiquitous Network Society. Several authors such as Brin and Bailey have therefore given up privacy as a workable concept altogether and instead stress the importance of transparency as a means to protect (individual) autonomy.[25] It is my expectation that in twenty years time there will be no more privacy; that is to say, physical barriers such as walls and fading memories will no longer afford privacy. Everything can and will be recorded and stored for future reference in the Ubiquitous Network Society. But that does not mean there will no longer be a need for privacy. The transformation of the public domain will force us to rethink our concept of privacy and come up with new methods for restoring privacy and safeguarding autonomy. Below I shall describe several ideas and concepts.

VI.1. Privacy by Design

Privacy by design is a design philosophy whereby privacy rules are incorporated in the design of an information system. By 'hardwiring' privacy rules into the technology, unnecessary 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 protection in itself, since rules can be broken or changed, whilst the design of an information system can force users to comply with the rules set forth in the design.

VI.2. Privacy as a Collective Interest

Currently, privacy is conceptualised as an individual right. However, the interests that privacy in the Ubiquitous Network Society aims to protect are actually collective interests (i.e. trust, autonomy, social cohesion and equal treatment). Thus, positioning privacy as an individual right may actually be counterproductive; the 'secretivism' 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

[25] D. Brin, *The Transparent Society*, Redding: Perseus Books 1999; D. Bailey, *The Open Society Paradox: Why the 21st Century Calls for More Openness, Not Less*, Washington: Potomac Books 2004.

society, discussions that position an individual's right to privacy versus the security of society as a whole can be avoided.

VI.3. Trust

Evidence suggests that when individuals perceive that others are behaving cooperatively, they are moved by honour and 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.[26] 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.

We have established that a lack of transparency is particularly likely in the Ubiquitous Network Society, where surveillance is for the most part a 'black box'. It is therefore extremely important to find ways to ensure trust in surveillance in the Ubiquitous Network Society. Proportionality, subsidiarity, judicial oversight and regular reviews of surveillance practices are absolutely necessary not only to ensure the legitimacy of surveillance practices, but also to foster trust in their application.

VI.4. Transparency and Reciprocity (by Design)

Even though privacy will remain an important right in the Ubiquitous Network Society, we must acknowledge the fact that in itself, privacy will be inadequate and possibly even counterproductive as a means to maintain personal autonomy. We have established that the main issue when it comes to surveillance in the Ubiquitous Network Society is information asymmetry: whilst the surveyors have access to all the information, the surveilled do not. This means that the surveilled are fully transparent, while the process of surveillance is not.

Therefore, authors like Brin and Bailey have looked towards (reciprocal) transparency as a means to negate information asymmetries. The idea of reciprocal transparency and the related notion of *sousveillance* are based on the premise that surveillance power should be equally distributed. Brin argues that the current distribution of surveillance power in society is unequal as it is concentrated mainly within existing power structures like the government and the major corporations. In order to restore this balance we must not try to hide information or ban the use of it through the right to privacy, but rather we must opt for full transparency using a *quid pro quo* system of surveillance. When an actor in society (a person, government agency, or corporation) wants to bring surveillance powers to bear against another, the

---

[26] D. M. Kahan, 'The Logic of Reciprocity: Trust, Collective Action, and Law', *Public Law and Legal Theory Research Paper No. 31*, Yale Law School 2009.

actor himself (or itself) must be submitted to the same form of surveillance. According to Brin, this approach will stimulate the equal distribution of surveillance powers, increase transparency and accountability, and lead to a more responsible use of surveillance powers.

While Brin puts forward a persuasive argument for reciprocal transparency, I believe Brin's transparent society is undesirable, due to the fact that it might lead to a tyranny of the majority over the minority. Another problem with Brin's idea is that it is almost impossible to distribute surveillance power equally amongst all. Surveillance is labour intensive and capital intensive, meaning most individuals cannot afford to use surveillance power in ways the more affluent individuals or institutions can. Moreover, governments and companies might have legitimate privacy interests as well (for instance those related to national security or competition), making reciprocal transparency virtually impossible.

However, this does not mean that we should discard transparency and reciprocity altogether. On the contrary, both transparency and reciprocity should feature far more prominently in the Ubiquitous Network Society to mitigate the risks of information asymmetries. In particular, we should remedy some the 'black box' nature of the Ubiquitous Network Society. While there are data protection rules in place that are aimed at increasing transparency, up until now the idea of transparency is not part of an actual design philosophy. This is important, since a major aspect of the design philosophy for pervasive computing systems in the Ubiquitous Network Society is that they should not burden the user. Ideally, the use of information systems should be unobtrusive and intuitive. But this design philosophy also makes the information systems less transparent. Therefore, an approach that entails that the data subject is granted maximum access to the acts of data processing in order to keep a form of reciprocity between the data subject and the company or institution using his data is necessary. We call this approach 'transparency and reciprocity by design'.

By creating tools and functional design guidelines for ubiquitous data processing we can create a greater degree of transparency and empower the user. Ideas in this area include: 1) easy mechanisms for accessing and querying databases associated with ubiquitous computing (for instance via agent technology), 2) tools for explaining/visualising automated decision processes, 3) setting forth rules for changing or removing personal data by the data subject, 4) the creation of log files that are intelligible for users, even without a deep understanding of the system, and 5) regular reviews of systems and applications.

Transparency and reciprocity are thus vital to retain and grow trust in surveillance in the Ubiquitous Network Society.

Conclusion

The technologies that will facilitate the Ubiquitous Network Society promise to greatly enhance our lives, making it easier, more comfortable and more efficient. These technologies will also enable the development of surveillance applications such as mirror worlds and augmented reality that promise to increase our security by providing law enforcement agencies with real-time data they need to become more efficient and effective.

However, the use of surveillance in the Ubiquitous Network Society is not without risks. Surveillance creates information asymmetries that lead to power asymmetries. Furthermore, reliance on surveillance data also heightens the risk of 'digital discrimination' and exposes individuals to the risk of false positives. These risks are compounded by the fact that surveillance in the Ubiquitous Network Society will be far less transparent than it currently is. This can be attributed to three related factors: 1) there will be far more data available (in some cases provided by the data subjects themselves), 2) there will be more parties gathering and sharing information, 3) data gathering will be unobtrusive. Ultimately, this means that privacy as a 'physical property' will become a thing of the past, leaving us with privacy as a right. As I have argued in this article, the right to privacy by itself will not be enough to protect the autonomy of groups and individuals. The reasonable expectation of the privacy criterion and the law of criminal procedure will not provide adequate mechanisms to remedy information asymmetries. Therefore we need different mechanisms to ensure autonomy and privacy.

When it comes to protective measures to function alongside the right to privacy, trust and transparency should feature prominently. In particular the black box nature of the ubiquitous network needs to be remedied. To this end we need to establish some measure of reciprocity and empower the data subject. Creating tools and functional design guidelines for ubiquitous data processing can help reduce the privacy risks of the ubiquitous computing age.