TRAMES, 2012, **16**(**66/61**), 4, 369–381

# HOW DO VIOLATIONS OF PRIVACY AND MORAL AUTONOMY THREATEN THE BASIS OF OUR DEMOCRACY?

**Katrin Laas-Mikko[1] and Margit Sutrop[2]**

*[1]Certification Centre Ldt., Tallinn, and [2]University of Tartu*

**Abstract.** Behavior detection technologies are currently being developed to monitor and manage malintents and abnormal behavior from a distance in order to prevent terrorism and criminal attacks. We will show that serious ethical concerns are raised by capturing biometric features without informing people about the processing of their personal data. Our study of a range of European projects of second-generation biometrics, particularly of *Intelligent information system supporting observation, searching and detection for security of citizens in urban environments* (INDECT) and *Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces* (ADABTS), shows that violations of privacy put several other values in jeopardy. We will argue that since privacy is in functional relationship with other values such as autonomy, liberty, equal treatment and trust, one should take this into account when limiting privacy for protecting our security. If indeed it should become necessary to restrict our privacy in specific situations, thoughtful consideration must be given to other ways of securing the values that form the foundation of our liberal democratic society.

**Keywords:** values, privacy, security, autonomy, democracy, second-generation biometrics, behavior detection, surveillance, function creep, INDECT, ADABTS

**DOI:** 10.3176/tr.2012.4.05

## 1. Introduction

Privacy is an important value, but protecting it continues to become more difficult. One reason is that another value, security, seems to be increasingly in danger, and its defense appears to demand significant curbing of privacy. The high rate of population growth, significantly increased mobility, and the development of information and communication technologies entail the elevation of security to the position of supreme value, in the name of which people are willing to limit privacy or relinquish it altogether.

In the context of such noble goals as creating a safe world, the protection of privacy may well turn out to be illusory. There are numerous predictions that the "Fight against terror 'spells the end of privacy'" (Travis 2009). Several recent trends and government initiatives which aim to enhance the capability for surveillance and detecting potential criminals or terrorists also feed growing apprehensions that the future may not bode well for the right to privacy.[1]

The problem is that what is being endangered is not really privacy alone; since privacy supports a range of other values, limitations on privacy can also place these other values at risk. As pointed out by several authors (Gavison 1980, Kupfer 1987, Solove 2007), privacy promotes liberty, autonomy, selfhood, and human relations, and furthers the existence of a free society. Therefore, in a democratic state one should continually be posing the question, what is the price of protecting security? The main purpose of our paper is to urge upon us the need to weigh carefully whether we are actually willing to relinquish privacy and a host of other values in the name of security. Of course, security is a crucial matter, but the means we use to ensure it should be proportional to the greatness of the potential threat. We should also consider whether those values that have previously been maintained by privacy can be protected in some other way.

Indeed, it is paradoxical that decisions are made to limit privacy in order to protect democratic society and ensure its security, while these same means of protection can erode that same society (more effectively than attackers might have done), by undermining its basic values. This reminds us of the satirical film, "Team America: World Police", where in the name of capturing a few terrorists, the Louvre and the Eiffel Tower are blown up, along with other landmarks essential to our culture.[2]

In what follows we will first analyze the concept of privacy, beginning with the functions it fulfils in liberal democratic societies. Subsequently, we will examine some specific examples of second-generation biometric projects which raise serious ethical concerns: behavior detection without informing people about the processing of their personal data violates not only their privacy, but also their moral autonomy and other values. The aim of this paper is to show that we should not give up our privacy too easily; after all, privacy is a necessary condition of autonomy and democracy, without which our society will lose its foundation.

---

1 For example see the following with regard to cellphone surveillance in the US. http://www.nytimes.com/2012/07/15/opinion/sunday/the-end-of-privacy.html, security laser scanners used in airport controls http://washington.cbslocal.com/2012/07/11/new-homeland-security-laser-scanner-reads-people-at-molecular-level/ etc.

2 "Team America: World Police" Details 2004, USA, Cert 15, 98 mins, Animation/Satire, Dir. Trey Parker.

## 2. The value of privacy

Privacy can be described as limited to the 'sphere' surrounding the person, within which that person has the right to control access to himself or herself. Consequently, privacy is applicable only within certain boundaries (not necessarily or only spatial) that surround that person (Persson and Hansson 2003:61). We support a normative concept of privacy, where privacy means the person's right to decide who and to what extent other persons can access and use information concerning him or her, have access to his or her physical body; access and use physical/intimate space surrounding the person.

Privacy can be an intrinsic value, while also fulfilling many important goals. In her article "Privacy and the Limits of Law" (1980) Ruth Gavison has shown that when speaking of the functional/instrumental meaning of privacy, we begin with the assumption that privacy is concerned with developing or preserving something that is desired. Gavison distinguishes between functions that privacy has with respect to the individual and those that concern society as a whole. In order to determine what functions privacy has with respect to the individual, we must consider what we deem important about being a person. Many Western theorists (Gavison 1980, Kupfer 1987, Häyry and Takala 2001, Rössler 2005) have indicated that the primary task of privacy with respect to the individual is to protect his or her autonomy. For example, Joseph Kupfer (1987:81–82) claims that privacy is a necessary (though not the only) condition for the development of an autonomous 'I' or self. One of the most thorough treatments of privacy has been presented by Beate Rössler in her book, "The Value of Privacy" (2005), which centers on the question of why we value privacy. Rössler endeavors to show that "privacy in liberal societies is valued and needed for the sake of individual liberty and autonomy, that is, for the sake of both freedom for each individual to fulfill himself, and thus ultimately for the sake of a life that is rewarding" (2005:44). She describes privacy as the ability to control 'access' in the physical or metaphorical sense to one's personhood, enabling autonomy practices; to decide over matters that concern one (including free behavior and action, that is, decisional privacy), to control what other people can know about oneself (informational privacy), and to protect one's own space for self-evaluation and intimate relationships (local privacy). In the context of development and application of new technologies, our main concern is with informational privacy, a person's control over the access and use of information about himself or herself.[3]

The answer to the question, what kind of society we desire depends on what we believe to be important to live a good life. Society should create opportunities for the flourishing of the individual. Preconditions for the self-realization of the autonomous individual are a liberal democracy and a pluralistic society, where everyone can live according to his or her chosen model of the good life. The reverse is also true: a democratic society presupposes an autonomous individual

[3] See Adam Moore's (2008) similar definition of informational privacy.

who can determine what constitutes the good for himself or herself and to choose the means of achieving this.

However, one should not only be able to determine what is good for oneself, but also the common good we all share. Collective benefits – security, peace, order, justice – pertain to all members of society and their existence depends on reciprocity. The question is, how should the common good be defined, as there are all kind of obstacles standing in the way of attaining it, such as subjective interests and continuous competition about scarce external goods. There are also differences in the extent of individuals' abilities to participate in deliberation on what should be understood as the common good.

Our suggestion is to learn from Aristotle's persuasive effort to bind together the common good and autonomy. The ground of Aristotle's political philosophy is his belief that "the state is by nature clearly prior to the family and to the individual, since the whole is of necessity prior to the part" (Aristotle 1996:1253a19) but neither stands independently of the other. The good of the republic is imbricated with the good of each citizen and the citizens experience the goodness of their republic in their everyday lives. For Aristotle the common good refers to "a good proper to, and attainable only by the community, yet individually shared by its members" (Dupré 1993:687). It was assumed that in normal situations the common good and the good of the individual would coincide. In case of conflict, the common good would be treated as the higher good.

Aristotle recognizes the conditions of the common good in both the virtuous character of the citizens and the institutional arrangements in the republic. Since the common good requires a shared life devoted to cooperative activities, it requires citizens to be just. Unfortunately most human beings are not just; they are perpetually engaged in competition for such external goods as honor, money or power. As there is always a scarcity of external goods, bad dispositions lead to intense competition and continuous conflicts. Consequently the main condition for arriving at the common good is the citizens' moral reorientation, which in turn implies education toward virtue.

Whereas in *Nicomachean Ethics* Aristotle teaches us that the common good cannot be achieved without the cultivation of the citizens' virtue of justice, in *Politics* he shows that it is essential to ensure constitutional arrangements which tie the good of the individual citizens to the good of the republic. Likewise it is imperative to involve all citizens in political deliberation concerning that good, which is attainable by the community, yet individually shared by its members. Deliberation about our collective ends requires practical reason (*phronēsis*), which is developed through self-governance in one's household affairs and through participation in political deliberation (Aristotle 2002:1141b23–1142a30). He reminds us that at the heart of politics there lies "a quest to protect the integrity and political autonomy of each citizen in a political cosmos" (Terchek and Moore 2000:911).

We think that Aristotle has convincingly shown that participatory self-rule is the highest political goal in itself; citizens' autonomy and common good are bound

together. If common good is not defined through reasoned deliberation about our collective ends, there is a great danger that under the guise of common good, power groups such as businessmen, politicians or security people may promote their private or sectarian interests. It is through participation in a reasoned, deliberative politics that we settle our differences and develop agreement about collective ends.

Here we come to the problems that occur when, without including people in the discussion, one value is chosen and set up to be higher than the others. For example, if without consulting the people it is decided that the primary value to be protected is security, in the name of which all other values are sacrificed, then the principle of moral autonomy is being violated. If violation of privacy is seen in the ordinary way as only the violation of individual rights, then what we see in reality is that by limiting people's autonomy we also damage the functioning of democracy, which is required for the full self-realization of persons. Ruth Gavison has pointed out that "Privacy is also essential to democratic government because it also fosters and encourages the moral autonomy of the citizen, a central requirement of a democracy" (1980:455).

## 3. Case study of second-generation biometrics technology: security *versus* privacy

To show that these theoretical ideas have practical relevance, we shall proceed to focus on the specific technology and show the context of its implementations in two projects, INDECT and ADABTS which are funded by the Seventh Framework Programme of the European Union. In these projects, behavior monitoring and detection technologies are researched and developed in order to prevent terrorism and crimes in public places. One of the technologies used in these projects is second-generation biometrics.

In general, biometrics is a tool used to identify and reliably confirm an individual's identity on the basis of physiological or behavioral characteristics (or a combination of both), which are unique for a specific human being (FIDIS 2009a). Such characteristics include facial image, fingerprints, hand geometry, the structure of the retina or iris, DNA, gait, heart pulse, and voice. First-generation biometrical systems have been focused mainly on the question "who are you?", linking a person's different identities to his or her physical identity and thus serving the first aim of distinguishing one person from the others.

New emerging biometric technologies, called next-generation or second-generation biometric technologies, have a more ambitious aim: detecting "which person you are", based on an automatic interpretation or decision about the person, and resulting in a classification. The decision is made on the basis of some predetermined indicators of abnormal behavior that justify placing the person in a category of suspects, which pose a potential threat or risk to the society (Sutrop and Laas-Mikko 2012:22). Second-generation biometric systems are focused on

intricate behavioral patterns, as indicated by gait or movement of the body, or by biological traits, states, and conditions of the body (e.g. heat, smell, ECG etc); using these patterns, the aim is to profile people on the basis of predictions of their actions and behaviors (McCarthy 2012).

Second-generation biometrics for security purposes is under development and testing; there are few available public materials about results of such projects and trials, since these are kept confidential. EU has initiated some behavior detection research projects such as INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environments), ADABTS (Automatic Detection of Abnormal Behavior and Threats in crowded Spaces), SAMURAI (Suspicious and abnormal behaviour monitoring using network cameras for situation awareness enhancement) etc. Let us proceed to a brief introduction to the INDECT and ADABTS projects. Our aim is to show, based on these examples, how second-generation biometrics technology implicitly relinquishes privacy and a host of other values in the name of security.

### *Intelligent information system supporting observation, searching and detection for security of citizens in urban environment (INDECT)*

The main aim of the INDECT project[4] is to develop new, advanced and innovative algorithms and methods aiming at combating terrorism and other criminal activities, such as human trafficking and organized crime which affect citizens' safety (INDECT 2012a).

In order to achieve this aim, the project foresees the development of the following items:

1) an intelligent information system for automatic detection of threats and recognition of criminal behavior or violence (with intelligent cameras);

2) tools for threat detection in the Internet (this includes the development of a new type of search engine combining direct search of images and video based on watermarked contents etc);

3) techniques for data and privacy protection in storage and transmission of data.

The INDECT project encompasses threat detection in physical environments with intelligent cameras (streets, airports, football stadiums etc.) and in virtual environments (including computer networks, Internet, social networks such as Facebook, chatrooms); algorithms enable the automatic analysis and extraction of the 'abnormal behavior' that can advert to a possible crime or terrorist attack. According to the homepage of the INDECT project, the methodology aims, first, to detect specific crimes such as bomb attacks, robberies, Internet child pornography, and trafficking of human organs, and then to detect the source of the identified crimes (for example, specific criminals responsible for the crimes). Abnormal behavior definitions are not clearly articulated and proven in this project; some behavior patterns in physical environment such as forgetting

[4] The homepage address is the following: http://www.indect-project.eu/.

luggage, rushing through the crowd, moving in the wrong direction, sitting too long in the airport, etc. are marked as suspicious (INDECT 2012b).

The prototyped information system will integrate different algorithms and technologies for abnormal behavior and databases with information for object recognition (car license plates) and the identification of persons. Automatic recognition of criminals and/or atypical situations and people, their parametric modeling and description, as well as systems for data processing and mining will be developed and combined in order to build a large network-oriented security system that should assist security operators (INDECT 2012c).[5]

### *Automatic Detection of Abnormal Behavior and Threats in crowded Spaces (ADABTS)*

The ADABTS[6] project aims to facilitate the protection of European Union citizens, property, and infrastructure against threats of terrorism, crime, and riots by means of the automatic detection of abnormal human behavior (ADABTS 2012).

Similarly to INDECT, the ADABTS project is designed to enhance surveillance and security by exploring the possibilities for automated operator support. This is based on the imagery of abnormal behavior or unusual events, where 'interesting' imagery can be distinguished. The extracting operations rely on signal-processing algorithms that detect predefined threat behaviors and deviations from 'normal behavior'. For real-time evaluation and detection of 'interesting' imagery, data from audio and video sensors are to be combined with context information. Operators would be alerted only when suspicious cases are detected, and they would then consider further decisions on whether or not to take some action. The abnormal behavior detection system will be used to monitor and secure some events or critical infrastructure such as international airports that are vulnerable to terrorist attacks and criminal activity (ADABTS 2012).

For our purposes it is important to understand what kind of imagery qualifies as 'interesting'. The aim of the ADABTS project is to arrive at a definition and create a list of indicators of abnormal behavior, as well as behavior models for scenarios in specific contexts – large-scale events, crowded public spaces, and critical infrastructure. So far, distinct and visible behavior, such as whole-body behaviors (including movement about a space, excessive body gestures or gait), have been identified as well as behaviors that are less obvious (such as signs of stress, eye movements, mumbling and sweating) (ADABTS 2011). In keeping with the ideas of the ADABTS project, some examples of abnormal behavior are rushing through the crowd, using an emergency exit, changes in heart rate, sensing body temperature changes, and others. Although there are many more criteria and types of suspicious behavior and abnormal physiological indicators, project participants

---

[5] See also disputed video about aims of the project is available at http://upload.wikimedia.org/wikinews/en/3/39/INDECT-400px.ogv.

[6] See homepage: https://www.informationsystems.foi.se/~adabts-fp7.

have not made these public for security reasons (Heck 2009). Preliminary tests on the ADABTS system have begun, and a final demonstration of the ADABTS system is planned at ADO (Alles Door Oefening) Den Haag in 2013 (ADABTS 2012).

## 4. Ethical values at stake

Implementation of second-generation biometrics in security contexts is intended usually for massive surveillance (or dataveillance); this means not only the monitoring of specific suspects, but placing all people who happen to be in public places under surveillance and scrutiny. It can be argued, that "… activities performed in public are explicitly being made public by the individual performing them, because the person would have the choice of doing something different and knows that he or she can generally be observed by others in public places" (ADABTS 2010). On the one hand it seems to be true that people can adapt their behavior under social control. But we have to admit that these kinds of technologies are more powerful than old (men-powered) systems and are accompanied by many new risks. As INDECT and ADABTS projects show, second-generation biometrics is integrated into larger surveillance systems, which make it easy to mine the data, to profile or match it by combining different data sources, and in this way to obtain additional information about the person. The biometrical data enables the creation of a profile of an identified person and to link other data to this profile. According to Helen Nissenbaum (1997; 2010), privacy in public places has to be protected, since in these kinds of cases of surveillance it is easy to transfer data from the context in which it was collected to another context and thus cause function creep.

The main ethical concerns about the application of second-generation biometrics are related to issues of privacy, autonomy, and equal treatment. Since this technology is used to survey persons' behavior in secured areas and detect abnormal behavior and events, as a result huge amounts of personal data are processed and collected into databases. Thus there are risks of data leakage or access by unauthorized persons, which means overriding the data subject's will about access and use of his or her data and therefore violating his or her privacy. How can privacy be violated if data is collected anonymously? Although in most cases the data collected will indeed be anonymous (the focus is not on *Who you are* but on the question *Which kind of person you are*), the problem is that it will still be possible to identify persons on the basis of comparing their video pictures with those in large databases, already existing in several countries (e.g. in Estonia there are large databases of e-passport pictures).

Is this a reason for concern? On the one hand we might indeed feel more secure if new methods are available for detecting criminals and terrorists and thus proactively prevent attacks on our lives. On the other hand, there is an increased possibility of stigmatization and discrimination on the basis of false interpretation of biometric characteristics. Behavior prediction based on the collection of biometrics and identification may lead to the social classification and stigmatization

of the person, placing him or her automatically in some category such as terrorist, criminal, unreliable or untrustworthy individual, etc.

In the case of second-generation biometrics, profiles are to be created about persons, and some people will be sorted out on the basis of different measurements of bodily behavior. Measurements form the set of the data that are 'mined' to detect the unique patterns for a particular person. Behavioral biometrics is the result of profiling, in which a certain kind of image is created and attached to the person, and then matched against data that can be used to provide more complete profiles (FIDIS 2009b). The main problem with profiling, besides data protection issues, is that it contains a stereotype of a possible offender, and this stereotype can inherit content from stereotypes of groups against which there is popular prejudice – and which is not evidence-based (Detecter 2008). The surveillance, as involved in behavioral biometrics, is according to David Lyon (2001) a form of social sorting, of categorizing persons and groups, which accentuates differences and reinforces the existing inequalities. We agree with Lyon that, unfortunately, these categories are seldom subjected to ethical inquiry or democratic scrutiny, despite their consequences for opportunities and choices in life. The reliability of these algorithms is under suspicion because of the high risk of a false error rate and a large number of fixed 'false images' of persons. "'Behavior' is a loose and socio-politically contingent concept," as Juliet Lodge (2010:8) points out. She claims that "defining a certain type of behaviour as deviant or indicative of 'risky intent' leaves behavior subject to the arbitrary interpretation, political vagaries, politico-ideological preferences and goals in power /…/." In this context, the following warning should be taken seriously: "Categories, descriptions and models are routinely imposed on individuals' identity information. We know what dramatic consequences the availability of labels like 'jew,' 'hutu,' 'tutsi,' and 'white,' 'black' and 'colored people' in administrative management systems can have for those concerned" (Manders-Huits and van der Hoven 2008:2).

In addition to this problem of stereotyping through arbitrary interpretation of deviant or risky behavior, another essential feature of behavioral biometrics is that it allows on-the-move authentication or behavior identification. Traits such as the dynamics of facial expression or gait can be captured and analyzed covertly without any physical contact with the person and thus without his or her explicit knowledge and consent. Usually intentions are attributed to a person according to certain behavioral or physiological characteristics before this person has decided to do any harm. We agree with Manders-Huits and van der Hoven (2008:5–6) that this is problematic because it violates the person's right to be engaged in self-identification, the core of a person's moral autonomy. This argument follows from Bernard Williams's (1973) idea that respect for moral autonomy implies taking into account the other person's self-identification: we ought to understand the other person's aims, evaluations, attitudes, thoughts, and desires. In other words, if we assess the behavior of a person, we have to put ourselves in his shoes, taking into account his beliefs, motives and intentions, life projects, among other concerns. In the case of behavioral biometrics, identification of a person is

performed from a third-person perspective without even attempting to interpret that person's motives. Thus, from the ethical point of view, we believe that the main problem with behavioral biometrics is that it does not make any attempt to take into account the person's self-identification; the person's behavior or physical characteristics are interpreted and viewed without any deeper knowledge of the person's own point of view. Thus, it may well be that the person's intentions or desires are misinterpreted.

It might be argued that today's world has become so dangerous that sorting people into categories is much less problematic than suffering from the threat of terrorism. Nevertheless, we should critically assess the proportionality of these measures. It has been pointed out that the risk of terrorism is overestimated, and that it is often manipulated in order to strengthen support for surveillance-based methods (Gray 2003).

Massive surveillance and dataveillance violate both privacy and autonomy; as we previously stated, these are not only individual values but also central values for a functioning democracy. Implementation of second-generation biometrics also harms other important pillars of democracy, such as the presumption of innocence and general trust in society. Interestingly, experts in technical fields assert that behavioral biometrics is not invasive, since it does not require physical contact with persons. We find that capturing biometric characteristics from a distance is even more invasive. As one may not be aware of the fact that one's biometric features are being collected and analyzed, control over the processing of data becomes more and more difficult and everyday life begins to approximate a surveillance society – being watched by a Big Brother. The practice of large-scale surveillance causes a climate of general distrust in society and overall suspicion against everyone. These consequences are known to those who have lived in totalitarian societies.

On the other hand, it is both understandable and natural that when risks to security are perceived to be increasing, people are ready to give up (some of) their privacy. We cannot overlook the fact that privacy is not an absolute value to be protected unconditionally. However, in each particular case, the restriction should be well founded and proportionate to the threat posed. As concerns biometrics, the conflict between individual and collective values seems genuine. As a common good, security is usually undisputable; otherwise the loyalty of the critic will be rendered questionable. The main problems that are overlooked are who decides that biometrics is collected in order to protect the national security, how this decision is made, whether public discussion is enabled, whether or not all important stakeholders of society are to be included, and whether the implementation of biometrics as a security measure is proportional to the risks incurred.

What could we do in order to enhance security on the one hand and maintain privacy on the other hand? Usually it is suggested that privacy can be maintained by holding on to the requirement of informed consent and notification for the processing of the individual's data (Manders-Huits and van der Hoven 2008:4). The failure to honor autonomy is expressed by the failure to obtain individual

consent. In the case of behavior detection technology, it is not deemed possible to implement individual informed consent. As we have shown in our earlier article (Sutrop and Laas-Mikko 2012:25), it is understandable that the procedures of informed consent are not implemented in contexts of national security, defense, and law enforcement. However, this does not mean that one should not respect people's autonomy. Granted, one really cannot make the implementation of safety measures voluntary, nor ask each individual for consent before collecting data. But it is still possible to inform people of the collection and processing of the data, as well as of the purpose of these activities; thus one offers an opportunity for control and a measure of standing up for one's rights. In addition, so-called public consent should be solicited in the use of technology. Even in the case of technologies where people are not aware of being under surveillance, their autonomy can be respected by allowing them, in other contexts, to participate in public discussion concerning the benefits and losses accompanying the implementation of technology, and in decision-making about whether or not such technology should be adopted. In the projects discussed above, those implementing the projects have not analyzed the ethical and social consequences of the proposed technology. At least there are no materials available that would indicate such an analysis. There is an impending danger that once the technology reaches the implementation phase, there will be no more opportunities to analyze their possible influences nor to solicit public consent.

## 5. Conclusions

We have shown how important it is to understand the value of privacy. We began by showing that privacy is a mediating value, which protects other values. Then, we indicated that it is therefore dangerous to take the relinquishment of privacy lightly, even in the name of supporting safety. We often do not notice that in this process we are relinquishing or failing to protect many other values, both individual and social, all of which are foundation stones of our society. Indeed, we desire to support security, but this cannot be done at the expense of destroying the basis of liberal democracy. We must at least be prepared to admit that security can be defended only in a completely different kind of society where there is no respect for human dignity, autonomy, and equal treatment, where trust is not honored, but replaced by total control and suspicion. Do we really want to live in such a society? Does this fit with our understandings of what is required for the flourishing of the human individual and living the good life?

## Acknowledgements

We would like to thank Tiina Kirss for valuable suggestions and help with our English and Laura Lilles-Heinsar, Mari-Liis Tina and Tiina Randviir for careful

assistance with our paper. We also acknowledge the financial support provided by the European Commission FP-7-REGPOT-2009-1 Grant No 245536 and by the Estonian Ministry of Education and Research grant SF0180110s08.

Addresses:
Katrin Laas-Mikko
Certification Centre Ltd.
Pärnu mnt. 141
11314 Tallinn, Estonia
Tel.: +372 5114 223
E-mail: katrin@sk.ee

Margit Sutrop
Department of Philosophy
University of Tartu
Jakobi 2
51003 Tartu, Estonia
Tel.: +372 7375 314
E-mail: margit.sutrop@ut.ee

## References

Aristotle (1996) *The Politics*. Stephen Everson, ed. Cambridge: Cambridge University Press.

Aristotle (2002) *Nicomachean Ethics*. Roger Crisp, trans. and ed. Cambridge: Cambridge University Press.

Automatic Detection of Abnormal Behavior and Threats in crowded Spaces (ADABTS) (2010) "ADABTS WP3 abnormal behaviour. D.3". Available at <https://www.informationsystems.foi.se/main.php/ADABTS_D3.1_Abnormal_Behaviour_Definition_Public_%28PU%29_final.pdf?fileitem=49119233>. Accessed on 17.08.2012.

Automatic Detection of Abnormal Behavior and Threats in crowded Spaces (ADABTS) (2011) "ADABTS WP2 user needs. D.2.1". Available at <https://www.informationsystems.foi.se/main.php/ADABTS_D2%201_User_Needs_Final.pdf?fileitem=10010654>. Accessed on 17.08.2012.

Automatic Detection of Abnormal Behavior and Threats in crowded Spaces (ADABTS) (2012) Homepage. Available at <https://www.informationsystems.foi.se/~adabts-fp7>. Accessed on 17.08.2012.

Detection Technologies, Terrorism, Ethics and Human Rights (DETECTER) (2008) "D25. Moral risks of preventive policing in counter-terrorism". Available at: <http://www.detecter.bham.ac.uk/pdfs/D05.1MoralRisksofPreventivePolicingv2.pdf>. Accessed on 09.09.2012.

Dupré, Louis (1993) "The common good and the open society". *Review of Politics* 55, 687–712.

Future of Identity in the Information Society (FIDIS) (2009a) "D3.10. Biometrics in identity management". Available at <http://www.fidis.net/resources/deliverables/hightechid/#c2057>. Accessed on 17.08.2012.

Future of Identity in the Information Society (FIDIS) (2009b) "D7.12. Behavioural biometric profiling and transparency enhancing tools". Available at <http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.12_behavioural-biometric_profiling_and_transparency_enhancing_tools.pdf >. Accessed on 17.08.2012.

Gavison, Ruth (1980) "Privacy and the limits of law". *The Yale Law Journal* 89, 3, 421–471.

Gray, Mitchell (2003) "Urban surveillance and panopticism: will we recognize the facial recognition society?". *Surveillance & Society* 1, 3, 314–330.

Heck, Wilmer (2009) "EU to monitor deviant behavior in fight against terrorism". *Spiegel Online*, Published online: 21 October. Available at <http://www.spiegel.de/international/europe/0,1518,656468,00.html>. Accessed on 02.10.2012.

Häyry, Matti and Tuija Takala (2001) "Genetic information, rights, and autonomy". *Theoretical Medicine* 22, 403–414.

Intelligent information system supporting observation, searching and detection for security of citizens in urban environment (INDECT) (2012a) Homepage. Available at <http://www.indect-project.eu/>. Accessed on 17.08.2012.

Intelligent information system supporting observation, searching and detection for security of citizens in urban environment (INDECT) (2012b) "D7.2 Creation of event model in order to detect dangerous events". Available: <http://www.indect-project.eu/files/deliverables/public/INDECT_Deliverable_D7.2_v20100430_final.pdf/view>. Accessed on 17.08.2012.

Intelligent information system supporting observation, searching and detection for security of citizens in urban environment (INDECT) (2012c) "D7.3 Biometric feature analysis component based on video and image information". Available: <http://www.indect-project.eu/files/deliverables/public/deliverable-7.3/view. >. Accessed on 17.08.2012.

Kupfer, Joseph (1987) "Privacy, autonomy, and self-concept". *American Philosophical Quarterly* 24, 1, 81–89.

Lodge, Juliet (2010) "Quantum surveillance and "shared secrets": a biometric step too far?". In *Justice and home affairs. CEPS Liberty and Security in Europe*, 1–39. Available at <http://www.policypointers.org/Page/View/11489>. Accessed on 02.10.2012.

Lyon, David (2001) "Facing the future: seeking ethics for everyday surveillance". *Ethics and Information Technology* 3, 171–181.

Manders-Huits, Noëmi and Jeroen van der Hoven (2008) "Moral identification in identity management systems". In *The future of identity in the information society*, 77–91. Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, and Leonardo Martucci, eds. New York: Springer.

McCarthy, Paul (2012) "Biometric technologies". In *Encyclopaedia of applied ethics*. 2nd ed. Ruth Chadwick, ed. Amsterdam: Elsevier.

Moore, Adam (2008) "Defining privacy". *Journal of Social Philosophy* 39, 3, 411–428.

Nissenbaum, Helen (1997) "Toward an approach to privacy in public: challenges of information technology". *Ethics and Behavior* 7, 3, 207–219.

Nissenbaum, Helen (2010) *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, California: Stanford University Press.

Persson, Anders J. and Sven O. Hansson (2003) "Privacy at work – ethical criteria". *Journal of Business Ethics* 42, 59–70.

Rössler, Beate (2005) *The value of privacy*. Cambridge: Polity Press.

Solove, David J. (2007) "'I've got nothing to hide' and other misunderstandings of privacy". *San Diego Law Review* 44, 745–772.

Sutrop, Margit and Katrin Laas-Mikko (2012) "From identity verification to behaviour prediction: ethical implications of second-generation biometrics". *Review of Policy Research* 29, 1, 21–36.

Terchek, Ronald J. and David K. Moore (2000) "Recovering the political Aristotle: a critical response to Smith". *The American Political Science Review* 94, 4, 905–911.

Travis, Alan (2009) "Fight against terror 'spells end of privacy'". *The Guardian*, Published online: 25 February. Available at <http://www.guardian.co.uk/uk/2009/feb/25/personal-data-terrorism-surveillance>. Accessed on 05.10.2012.

Williams, Bernard (1973) *Problems of the self*. Cambridge: Cambridge University Press.