



EBERHARD KARLS UNIVERSITÄT TÜBINGEN

INTERFAKULTÄRES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN (IZEW)  
INTERDEPARTMENTAL CENTRE FOR ETHICS IN THE SCIENCES AND HUMANITIES



IZEW – Interfakultäres Zentrum für Ethik in den Wissenschaften  
Universität Tübingen · Wilhelmstr. 19 · D-72074 Tübingen

---

Wilhelmstr. 19· D-72074 Tübingen  
Tel.: 0 70 71 / 29 - 7 79 81  
Fax: 0 70 71 / 29 - 52 55  
e-mail: [izew@uni-tuebingen.de](mailto:izew@uni-tuebingen.de)  
<http://www.izew.uni-tuebingen.de>  
Arbeitsbereich Ethik und Kultur  
- Leitung -  
Prof. Dr. Regina Ammicht Quinn  
Durchwahl: 29 - 7 79 88  
[regina.ammicht-quinn@uni-tuebingen.de](mailto:regina.ammicht-quinn@uni-tuebingen.de)

*Prof. Dr. Regina Ammicht Quinn*

*Andrea Pabst*

## **Ethical Advisory Service for TeraSec: Report**

### *Contents*

- (0) Introduction**
- (1) Security**
- (2) Freedom**
- (3) Justice**
- (4) Privacy**
- (5) Conclusion**
- (6) Recommendations**
- (7) Selected Literature**

---

Vorstand: Prof. Dr. Eve-Marie Engels (Sprecherin) · Prof. Dr. Dr. Kristian Kühl · Prof. Dr. Dr. Urban Wiesing  
Wissenschaftliche Koordination: Dr. Thomas Potthast · Dr. Walter Schmidt  
Wissenschaftlicher Rat: Prof. Dr. Vera Hemleben (Vorsitzende) · Prof. Dr. Regina Ammicht Quinn · Prof. Dr. Georg Braungart  
Prof. Dr. Dieter Cansier · Prof. Dr. Eve-Marie Engels · Prof. Dr. Eilert Herms · Prof. Dr. Klaus-Peter Horn  
Prof. Dr. Robert Horres · Prof. Dr. Dr. Kristian Kühl · Prof. Dr. Dietmar Mieth · Prof. Dr. Martin Nettesheim  
Prof. Dr. Albert Newen · Prof. Dr. Olaf Rieß · Prof. Dr. Dr. Urban Wiesing

## **(0) Introduction**

Technologies are not ‘good’ or ‘bad’ in a moral sense of the word; as technologies, they are ‘good’ or ‘bad’ in a functional sense. Ethical reflection deliberates on questions of preconditions, purposes, and consequences of a technology’s production and implementation and on patterns of behaviour and visions of world these technologies imply.

If conflicts arise from the implementation of a technology, those conflicts are more than technical conflicts: They are conflicts about conceptions of the future, ideas of man, designs of society. To describe these conflicts and to search for ethically acceptable solutions is not an end in itself. Both the conflicts and the search for ethically acceptable solutions occur in a specific historical, social-political context. What is perceived as a problem and what may ultimately be perceived as a solution will always have political relevance.

An ethical analysis of technology implies a certain understanding of technological development. Technological development is not seen as a self-directed, self-contained evolution with little or no chance of intervention. Technological development is seen as a process which is intimately connected to the question about our natural and social environment and about the type of society in which we want to live.

The TeraSec project develops a new technology which will make it possible to detect threats, explosives, pathogens and chemicals hidden not only inside objects such as letters or luggage but also on a person. The new technology is based on THz radiation and advanced sensor concepts. THz radiation is transmitted by clothes and most packaging materials such as paper or plastics. In a ‘close-by detection system’ explosives and bio-agents hidden in close-by objects such as letters can be detected. In a ‘stand-off imaging system’ threats and explosives carried by a distant person (up to approx. 20 m) can be detected. In combination with existing sensors TeraSec thus aims to increase the level of security at public places. (<http://terasec.de>)

Terahertz technology is able to combine the *control of persons* (traditionally: manual control, metal detectors; new: millimetre scans, backscatter technologies) with the *control of spaces* (control by security personnel; CCTV). The digitalised image of the naked body is visible on the computer screen. The exposed body may also expose, for example, ceramic knives, plastic explosives, bio-agents, along with a person's bodily defects, prostheses, genital piercings – or in short, the normally well-covered very intimate, sometimes shame-related private, very own body.

Ethical issues in research were addressed in the “Information on the Ethical Aspects Regarding the Proposal *Active Terahertz Imaging for Security (TeraSec)*” as well as in the “Ethical Review Report” (Brussels, September 29<sup>th</sup> 2004, J.Prieur). To our knowledge the requirements were conscientiously fulfilled – e.g. the consent forms for research participants and the constant investigation of the current state of knowledge on potential risks and hazards associated with THz radiation.

Currently the primary intended places for the implementation of TeraSec technology are airports. Airports are not only symbols of mobility but also global spaces where world cultures with their own distinct traditions, beliefs, habits and fears meet in a defined space.

Conflicts that may arise with the implementation of TeraSec technologies are conflicts arising from different hierarchies of values, different cultural and religious traditions, and different conceptions of the good life. To analyse potential conflicts and to seek possible solutions the present report will reflect ethical concepts with regard to TeraSec technologies: (1) security, (2) freedom, (3) justice and (4) privacy. It also presents a conclusion (5) and makes concrete ethical recommendations (6).

## (1) Security

- *Concepts*

Am I going to be safe?

Are those around me going to be safe?

Are the things I value going to be safe?

These questions are common, because security is a fundamental concern for people and societies, especially Western societies.

Western societies are in comparison with many non-Western societies relatively secure. The subjective perceptions of security, however, are not automatically congruent with an objective and identifiable status of security. The feeling of insecurity may exist where there is no real threat to security. Likewise there may be a real threat to security in cases where people feel secure. For these reasons, in discourses on security the sense of security, the feeling of safety should always be considered in relationship to actual risks or threats to security.

In pre-modern times threats to security as well as provisions of security were attributed to nature, gods or demons. In modernity security is no longer understood as something that is either given or not given; it is the result of concrete action. Security has become the task of individuals as well as political communities. This task of providing security for an individual life, a family, and all citizens has a variable share of uncertainties and contingencies. The handling of security issues is an attempt to calculate something that can barely be calculated, if at all. The realisation of security cannot be taken for granted.

In post-modern societies this quest for security has intensified on the background of vast insecurities. These insecurities are caused by objective risks as well as by their political and media presentation. The globalized world has rendered political, social or ideological boundaries increasingly irrelevant. Threats to security are no longer bound and limited to

clearly defined spaces, times or social and national groups. Reasons for insecurity relate to a wide range of issues: ecological issues, financial crises and international terrorism affect the global world in a global way. Especially in the North, the 9/11 attacks and the subsequent attacks in Madrid and London left people with a feeling of deep insecurity even though the so-called developing countries are much more affected by the consequences of 9/11.

The more private and public lives are perceived as insecure, the more security becomes a highly emotionally and ideologically charged concept. 'Security', however, is no simple reality; it is a social fiction, at most a temporarily obtainable status, never a permanent attribute of life.

Security itself is a broad and in many cases indistinct concept. It is indistinct because of its multiple levels and subjective contents. Security thus appears as the "result of assumed certainties" (Glaeßner 2003: 18). The term 'security' applies to a wide range of issues: security of one's status; security of a political / social system; security of institutional arrangements (e.g. police, education); legal security; financial security; the reduction of risks; the reliability of expectations (Erwartungssicherheit). It also includes the whole realm of personal security: security in relationships, security of one's private life, security from health threats; security of a person's bodily integrity. These different facets of 'security' can complement each other, compete with each other, or mutually exclude each other.

Until recently, a rather narrow state-centered approach to security dominated the political discussion. Security was understood as providing order within a political community (police; law) and as protecting the national state from external (military) threat. This has to some extent been superseded by a broader approach. The UN Commission on Human Security defines security as "protecting the vital core of all human lives in ways that enhance human freedom and human fulfilment" (Commission on Human Security 2003: 4). The primary goal of security is more than just protecting people; it is enhancing human life.

### *Pursuit of Security*

The public pursuit of security shows two different and differently valued paradigms that are intimately linked: backward-looking reactive prosecution and forward-looking proactive prevention. There is a high priority on the latter. This is the field of TeraSec: It is a technology aimed at prevention.

The success or failure of a technology ultimately depends not just on its technical qualities but on a society's acceptance or rejection of the technology. Acceptance or rejection depend in part on how well a society can understand the technology, but in equal parts on how well the development and implementation of a technology shows an understanding of the society. The TeraSec project is a response to actual security challenges. It deals with risks and threats as well as with perceptions and feelings of security and with the fact that security is a highly emotionally and ideologically charged concept. This presents a twofold problem for security technologies:

(1) On the one hand, comprehensive security cannot be produced through technology alone.

(2) On the other hand, even those parts of security which can be technically established are subject to a vast range of contingencies that may affect the desirable outcome. Technologies themselves are not 'secure'; every technology can malfunction. Moreover, technologies are dependent on different agents (from governments to surveillance personnel) who, being human, can react to technical failures and correct them but, being human, can also be the source of errors and faults.

In consequence, security technologies cannot be seen as a means of creating 'security' as a comprehensive concept. *Security technologies are instruments for partially reducing risks.* It is socially and politically necessary to clarify and reduce the expectations in security technologies. Objective risks can be partially reduced with security technologies. At the same time, these technologies directly or indirectly influence the prevalent feeling of security or insecurity.

### *Ethics of Security*

Security programs and practices are not mere technical discourses, they are normative discourses. Different understandings and evaluations of security are based on different ideas of man and different concepts of a desirable future.

An ethical reflection of security will focus on two points; one is *specific*, one is *general*.

The security practice that is *specifically* concerned with prevention may be used not only against persons who have already been convicted of wrongdoing but also against those who might commit future crimes. Preventive security practice thus provokes questions of justice: If ‘those who might commit future crimes’ are defined as people with certain attributes, preventive security practice can take on the form of social and racial prejudices. If ‘those who might commit future crimes’ is everybody, then everybody is subjected to a general suspicion. Everybody is no longer innocent until found guilty, but guilty until found innocent.

In *general*, security is widely recognized as a fundamental value. It is, however, not necessarily and not appropriately the highest personal or political value. Security has to be weighed against other human priorities or values, first and foremost such as liberty, justice, and privacy. If the pursuit of security is not compatible with other central values, the ultimate goal of enhancing life can easily be missed. To achieve this goal, this balance between the pursuit of security and the pursuit of freedom, justice, and privacy has to be appropriate. In cases of conflicts between security and freedom, justice, or privacy, an appropriate balance might require rethinking security and/or the method employed to achieve it.

All human values and fundamental rights are subject to a constant process of balancing. Those values and rights compete with each other and can never be fully exercised all at the same time. The necessary constrictions of those values and rights have to follow clear rules:

The constrictions have to be necessary, adequate, and executed with the proper measure. These constrictions of human rights are, however, constricted themselves: A fundamental right can, morally and legally, never be totally erased in favour of other values. An ongoing social, ethical and legal discourse has to determine the necessary limits when fundamental rights are constricted.



## (2) Freedom

- *Concepts*

Freedom is the foundation of democratic states as well as the foundation of individual concepts of life.

Freedom does not primarily mean to minimize restrictions and restraints. Freedom means to have choices and to have the ability to choose life goals and life styles. Negative ‘freedom from’ which is not complimented by a positive and active ‘freedom to’ can lead to a negation of aspects essential to the very nature of human freedom.

If people do not live completely isolated lives, collisions of life goals and life styles are unavoidable. A central feature of a free society is to provide just solutions in case a person’s, a group’s or a state’s freedom collides with another person’s, group’s or state’s freedom. These just solutions often result in personal or social restrictions. These restrictions, however, are fundamental for safeguarding freedom in any society.

- *“Safety” and “Liberty”*

*Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.* (Benjamin Franklin)

In his famous admonition Benjamin Franklin refers to the basic conflict between safety and liberty – without answering the question, what the “essential” liberties are and what kind of safety is only “little” and “temporary”. It is clear, however, that for Franklin especially “safety” is not an absolute value but a relative one: relative to one’s liberty.

Liberty and safety can clash in different ways: In crisis situations, national states may restrict the freedom of individuals in order to protect the social community; considerate parents restrict their children's freedom of movement in order to keep them safe; communities might impair people's physical or mental mobility in order to save the community's identity. These actions of promoting safety are highly ambivalent: They can destroy "essential" liberties, but they can also facilitate freedom – e.g. when a safe environment allows the freedom of movement. If security is defined as "protecting the vital core of all human lives in ways that enhance human freedom and human fulfilment" (Commission on Human Security 2003: 4) then all practices that damage freedom, even with the best intentions, are also bound to damage security.

- ***Control and care***

The implementation of TeraSec technologies aims at heightening security through special methods of surveillance. The desired result is a maximum of freedom and a minimum of subjective fear and objective insecurity.

Surveillance is an ambiguous practice, situated between control and care. Children or people in hospitals are kept under surveillance, because they are cared for. Prison inmates are kept under surveillance because a genuine mistrust demands control. Concrete practices of surveillance are situated somewhere between those two poles. It is ethically relevant to determine the exact position of a certain practice.

- ***Ethics of security and freedom***

Externally, the practice of surveillance as control and surveillance as care can appear exactly the same. The difference lies in the *intention* which led to the development and implementation of the respective technology as well as in the *attitude* with which the task is performed. And the difference can lie, more often than not, in the specific *technical method*

of surveillance. Technical methods are not 'neutral' but sources of attitudes and patterns of behaviour.

With regard to TeraSec technologies the *intention* of any implementation can and should be to safeguard and not to repress people.

The *attitude* with which the task is performed cannot be easily determined nor can it be easily demanded or monitored. Professional surveillance personnel will be technically trained and legally authorised to do their work in a professional – exact and effective – way. Within the context of training, professionalism should include not just technical and legal aspects, but ethical aspects as well. Those using the new technology must be aware that what they do potentially intrudes upon one's personal space and interferes with one's personal rights.

The *technical method* of surveillance that reproduces the naked body's image on the computer screen is rather new and requires close scrutiny. A basic aspect of a person's freedom is particularly affected by the method of surveillance: the liberty to decide where, when and to whom a person's own body is exposed. Depending on cultural, social, religious backgrounds and individual mindsets this could be seen as a marginal, a severe or an absolute violation of a person's freedom. While some people might find comfort and freedom of mobility in heightened surveillance, others might be deeply offended, feeling expelled from the mobility this method of surveillance intends to protect.

### **(3) Justice**

- *Concepts*

Justice is a basic idea in all ethical concepts. It is the fundamental ethical principal for any social and political structure, and it is a personal virtue. As a personal virtue justice guides one's actions, even in situations where existing laws and customs may not offer guidance. Justice as a personal virtue can offer a safeguard against unjust developments in a society.

- *Ethics of security and justice*

With regard to TeraSec's future implementation questions of justice are particularly relevant in three areas:

**(a) The problem of social sorting / racial profiling**

Airports are key gateways of mobility. Here the flow of people and the flow of luggage and goods are monitored in order to guarantee a smooth sequence of actions and a maximum of security. With TeraSec, the surveillance of persons and the surveillance of spaces can be combined. Up to a certain degree, surveillance is always selective, dependent on technology, time pressure, attentiveness etc. Especially when spaces – e. g. entrance halls in airports – are kept under surveillance, it is self-evident that the surveillance has to be selective. An implicit or explicit process will decide where to focus one's attention. This selection process will be based on visual signs: If a person is, for example, young, male; black, Arab; shows visible signs of being Muslim; or if a person is visibly poor, the chances for closer scrutiny are high, regardless of the actual behaviour. Even if the surveillance personnel are aware of the problem of social sorting and racial profiling, it can hardly be avoided. Practices of surveillance can be, even if there are rules and good intentions, partly or totally practices of discrimination. The use of the technology can give way to common prejudices that classify people in worth/unworthy, legitimate/illegitimate, wanted/unwanted. This is a matter of social justice.

**(b) The problem of asymmetries**

Surveillance is based on a normally hidden social interaction. In most cases it is a one-sided relationship, with the person doing the surveillance acting as a subject, the person under surveillance being the object.

In TeraSec technologies the surveillance has a classically asymmetric structure. The observed is neither able to look inside her or his 'profile', nor is the person able to see who is doing the profiling.

In addition to the potential injustice arising from the asymmetrical surveillance structure, the body as the particular object of surveillance is a potentially great source of prejudice and further injustice. In every cultural context the body has a particular value; visual representations of the body are never neutral or value-free. The 'naked' body readily becomes an object of ridicule and denigration or the object of hidden desire, or often both at the same time.

**(c) The problem of global injustice**

The implementation of TeraSec will be expensive. It is a security technology most likely not all countries will be able to afford. Thus the acquired security would be reserved to rich countries. Poor countries could be forced to spend money on security which might not be available to meet other social needs, for example health, education, environment.

## (4) Privacy

- *Concepts*

Personal privacy can be understood as (a) immunity from the judgment of others; (b) the ability to control who has information about us or who has access to us, both physically and mentally (cp. Dandekar 1993); privacy means (c) to retain control over important decisions concerning the 'private sphere', e.g. family, relationships, lifestyle.

Privacy is not a luxury, but a necessity. This is most obvious in the case of people living almost constantly in public spaces like homeless people. They, too, need privacy. Privacy is necessary to define oneself in relation to others. Without a certain quantity and quality of privacy we are not able to build up relations with others. Social and public life would not be possible.

Even though the respective understanding of privacy differs throughout the world, privacy is always valued. In constitutional states with a clear separation of powers the right of privacy is at the core of the basic freedoms that are to be secured by the state. There, privacy is not only a psychological need but a fundamental right. Freedom of speech, of thought, of association, to name just a few, are grounded in the idea that there is a private sphere of thought and action that cannot be disturbed or destroyed by others. The right not to be known against our will, the right not to have to weigh every action, every statement, every human contact, wondering what a public would make of it, is at the core of human dignity, autonomy, and freedom. The right to privacy is, at its heart, the respect that society pays to the inviolability of the individual.

Airports, presumably the central places for TeraSec's implementation, are intercultural public places. An international airport is a particular microcosm, a global space where different cultures meet in a small place. At the same time the social mix that occurs at an airport is limited. Even though the percentage of people who can afford to travel by air is

large and growing, in a larger context the group of people using an airport still represents a very select, well-to-do group.

What is understood as an intrusion into privacy differs widely in different cultures. In Thailand, for instance, even the word for 'privacy' comes from the English as the Thai culture used to be much more collectively oriented than 'Western' societies. Similar arguments are made for China or Japan. Privacy in some cases refers first of all to the family and not to individuals. A right to privacy might then mean not only to decide who has access to information about a person but about the family whose representative this person is. This means at the same time that an intrusion into the privacy of a person has an impact on relatives or the community as well. In less individualized societies, therefore, privacy is not a lesser problem than in Western, highly individualized societies; privacy merely has another focus.

In a globalized world, what we perceive as 'Western' concepts of privacy has found its way into 'non-Western' contexts. But 'Western' concepts of privacy are far from being generally valid. As societies are pluralistic in themselves, different perceptions of privacy exist simultaneously within one culture.

- ***Security and privacy***

Security and privacy have a complicated relationship. Providing safety for people and securing the privacy of people might be even contrary goals. In private economy the collection of customer data can help to ensure financial safety and privacy; at the same time, these data can be used to breach privacy, when spending or traveling habits are analyzed and used for aggressive personalized advertising. Gated communities provide a maximum of security for their residents, who are, in return, put under constant surveillance. Providing and protecting privacy thus is by no means a clear-cut task.

In the light of extensive individualization in ‘Western’ societies, the appropriate balance between privacy and security is increasingly difficult. As people became more and more detached from traditional communities, individuals are more and more uncertain about the behaviour of others. Confidence in technology-based security measures tends to replace faith in other people. Whereas privacy concepts are more and more individualized, a growing number of people are willing to allow for intrusions into their privacy: “Surveillance [...] literally fills the gap created by an explosion of privacy” (Bogards 1996: 148).

Privacy is a highly cherished concept in contemporary ‘Western’ societies: There are locks on the doors and firewalls in the computer. At the same time we live in a political situation where the insistence on privacy raises suspicions: If an individual claims his or her right to privacy, he or she could have something to hide. And mostly, there is something to hide. Not necessarily because it is criminal, but because it is ... private.

- ***Identity***

Voice recognition as well as collection of biometrical data like fingerprints or iris scans are supposed to verify the identity of a person – “bodies become coded and function as passwords” (Aas 2006: 143). Here, identity is the sum of binary codes. TeraSec technology is not interested in a person’s identity or the body per se; it does not focus on persons; it focuses on objects that can be hidden on persons and aim at harming other persons. This only secondary interest in the body, however, has implications for a person’s identity.

Identity is more than a binary code as defined by biometric data collection. Identity is the social process where self-perception and how others perceive you is negotiated. A person’s identity is always bound to a physical body. The suspension of privacy in the sense that one cannot control who has access to oneself and especially to one’s very own body has a strong impact on identity.



The digital representation of the naked body takes place as a social interaction between the observer and the observed; this social interaction is part of identity construction. Even if the gaze of the observer on the naked body is not a face-to-face-interaction and the observer is ideally not interested in the body at all, social norms come into play at least in the perception of the observed. The knowledge of being observed influences the behavior of the observed as diverse studies about video surveillance have shown.

Because the observer is not a machine but a human being, he or she is socialized with certain norms and values. Being observed thus is perceived as being judged according to social norms; being judged might easily result in being shamed. Shame can occur because showing the naked body is culturally or religiously confined to the private or intimate sphere. It can be multiplied if this exposure is culturally or religiously forbidden; shame then will be perceived as guilt. In every case a person's identity is potentially challenged.

- ***The core of Privacy: Intimacy***

The most striking morally relevant aspect of TeraSec is the intrusion not only into private affairs but into the very core of privacy: the intimacy of the naked body. In the vast majority of cultures nudity refers to the most intimate, most private sphere. Being naked in public is unthinkable or at least very exceptional. Not surprisingly, the mapping of naked bodies by similar security technologies using backscatter or millimetre radiation has produced critical objections by civil society initiatives. Newspaper journalists first and foremost emphasize this outstanding feature of these security technologies when applied to scan people. In awareness of this problem, software tools are being considered that allow for an automatic identification of intimate body parts and make them indistinguishable. Apart from the practical reduction of security, this solution leads to more questions. It is not simply obvious what intimate body parts are. The perception of what are the body's intimate parts varies with social, cultural, age-related and religious contexts.

Bodies that do not fit an existing social norm can be found objects of shame that have to be concealed. The intimate body parts can be those which are perceived as not 'good' enough. For people with disabilities the question of privacy and intimacy can be even more difficult. With TeraSec technology, amputated body parts, prostheses, artificial anuses or problems of incontinence (in Germany alone up to 10 million people are affected by incontinence) are easily visible. People with certain disabilities often experience their bodies as objects accessible to others during their entire lifetime. Intimacy thus seems to be a privilege of 'normal' bodies. This experience can be reinforced and worsened by TeraSec.

What is defined as intimate body parts also differs due to cultural or religious belongings. This is probably most obvious in the case of Islam. The Quran and especially diverse hadith give orders for proper clothing. These orders are certainly debatable, but it still means that in a strict interpretation women should only show their face and their hands whereas men need to cover from the belly button to the knees - at least when being in public places. Complete nudity is unthinkable within Muslim communities. Although in Islamic law the prohibition of nudity can be deferred in favour of other commandments such as the protection of life, in everyday life the prohibition of nudity could result in a constrain of mobility – most likely especially for Muslim women.

If TeraSec is used as addition to CCTV scans, this could mean for some people not a new freedom through better security but an unacceptable intrusion of one's privacy – up to the point where people feel excluded from such places because they cannot accept this intrusion into their privacy for religious, social or cultural reasons. Used in wide area scans, TeraSec cannot ensure gender segregation. This again affects especially Muslim communities because the gender segregation in public places, provided by clothing that covers the body, is at the core of Muslim self-conception.

- *Ethics of security and privacy*

Balancing the values of security and privacy is extremely difficult. Basic rights can be restricted in favour of another right but they can never be completely suspended.

TeraSec aims at providing security through techniques of prevention. In the possible combination of the control of persons and the control of spaces (CCTV plus THz rays), TeraSec shares the problems of CCTV surveillance: questions of effectiveness, actual effects, human errors, questions of data handling, questions of racial and social profiling, questions of misuse and abuse. Beyond that, with THz rays the surveillance technology has an even deeper impact on privacy: Not only a person's actual conduct in a certain place is recorded, but also his or her naked body. For some people this can be perceived as an absolute destruction of privacy and identity.

To protect and safeguard children from harm is certainly more important than the privacy of people who do this harm. But it is not always so simple: Do we protect children from potential harm? Probable harm? Or certain harm? Do we take into account that absolute security is not possible?

In a situation where there is a clear urgency, a clear and concrete threat, a decision for safety and against privacy might be morally justified. If the urgency, however, is not clear or if, for example, the cause for action is only a general feeling of insecurity or fear, this justification would decrease.

A society in which privacy is a dispensable thing, subject to individual and collective fears, would not be able to enhance freedom and fulfilment. It would be a society where human dignity and autonomy are only secondary issues. And it would therefore be a society that denies itself the critical capability to examine carefully which values are balanced in which way against other things we value.

## (5) Conclusion

- Ethical reflection on technology

Conflicts that arise with the development and implementation of technologies are not mere technological conflicts; they are conflicts about conceptions of future. An ethical reflection on TeraSec technology is concerned with the obvious issues which are already present during research and development: health issues, data handling, privacy issues. In developing implementation scenarios for both Terahertz portal scanners and Terahertz wide area scanners, the problems with data handling and especially with privacy issues intensify – up to a point where a possible gap between the technology's intention and the technology's effects becomes visible.

- Foundation of ethical reflection

The foundation of the ethical reflection on a specific security technology is a critical analysis of concepts of 'security' itself. Total security is a fiction. It is a strong fiction in societies or situations where feelings of insecurity (not necessarily congruent with actual risks) are widespread. Security technologies do not provide security: They are instruments for partially reducing risks.

- Appropriate balances

Security is a fundamental value for most people and societies. In most cases it is viewed not as an absolute value, but rather as relative in relation to other values. It has to be weighed and balanced against other values – especially freedom, justice, and privacy. Problems that arise in this balancing process are, among others, the intrusion into the personal freedom to decide who has access to the own body; problems of intrusions into privacy where concepts of privacy vary according to age, social status, religious belief or cultural affiliation and thus are violated in various ways; violation of justice where social sorting and racial profiling are part of the surveillance process or where security standards in global air travel could be distributed according to financial power.

- Fundamental values, fundamental rights

Fundamental rights are never totally realized at the same time. Fundamental rights are bound to be constricted in some way, because fundamental rights can be competing with each other.

A fundamental right, however, can morally and legally never be totally abandoned in favour of other rights or values. Thus the fundamental right to privacy – as individual and social necessity – can in ethical and legal judgements never be forsaken as a whole in order to achieve security.

## (6) Recommendations

- (1) Health issues should be continuously addressed. Even if the present research and information show no negative effects on a scanned person's health, EU-wide safety regulations should be established and regularly checked.
  
- (2) The personal data acquired through a scan are images of a person's naked body. These are especially sensitive data, considering possible misuse and abuse. Misuse and abuse scenarios are among the strongest objections when TeraSec technologies are discussed. When TeraSec is implemented, no data should be stored. The goal of increased security can be obtained with live pictures. For some groups of people, however, pictures of their naked body – without data storage or possible data abuse – is seen as an abuse in itself. This presents a new dimension for questions of personal rights. A new European law to regulate the handling of these sensitive data is required.
  
- (3) If Terahertz rays are used for the entrance security check (portal scanners) in airports:
  - An alternative security check (metal detectors, manual control) has to be offered; people who choose the alternative check should not be placed at a disadvantage or put under suspicion. Security personnel should be aware of a wide range of reasons for choosing the alternative/traditional security check – not just criminal or terrorist ambitions. The decision of rather being manually searched or preferring the visualization of the naked body for security reasons is a very personal one and should be open to everybody.
  - Terahertz scans should never be applied without understandable and complete information and some form of consent.
  - The security personnel should have essential ethical training. Their performance should be supervised regularly, not only with regard to effectiveness and thoroughness, but also with regard to their social interactions in a highly sensitive field.
  
- (4) If Terahertz rays are used in combination with CCTV (wide area scanners):
  - Research into post-processing of data (not the naked body is visible, but only the hidden objects; there is no image but an auditory signal) should be intensified. This would be also a

big advantage for portal scanners. But with wide area scans, there are no alternatives of checking, e.g. a manual security check. ‘Privacy software’ that automatically covers intimate body parts on the screen is no solution – neither for safety, nor for privacy reasons.

- If the post-processing of data is not yet possible, the use of Terahertz scans should be limited to situations with a special urgency and a special risk profile. Authorities and procedures to determine the urgency and thus the moral justification of an intrusion into a person’s privacy have to be established.
- Terahertz scans should never be applied without understandable and complete information and some form of consent.
- The security personnel should have essential ethical training. Their performance should be supervised regularly, not only with regard to effectiveness and thoroughness, but also with regard to their interactions in a highly sensitive field. This is necessary to prevent misuse of the technology that can occur already without any data storage.
- Even with some kind of post-processing of data in place, people with certain disabilities are most likely still being set apart and discriminated. The technical selection might not be avoidable; it should never become tantamount to social discrimination. An awareness of this problem – which might also occur at the personal security check – and an empathetic and responsible answer to it is absolutely necessary.
- Gender segregation in public places that is at the core of Muslim self-perception is not possible in wide area scans. It cannot be guaranteed that only women scan women, and scanning somebody in a crowd would always mean to have at least parts of other people on the screen as well.

(5) If Terahertz scans are implemented, accompanying research on data handling and health issues, but especially on possible social/political impacts is highly recommended.

(6) Terahertz technology has also to be considered as potential merchandise. Its sales, however, should be restricted to ‘trusted customers’. Authorities and procedures to confirm the trustworthiness of a customer have to be established.

- (7) A public discourse on TeraSec where different voices can be heard is required. It should include all scanning technologies where the naked body is displayed. This public discourse is open-ended and would take into account possible advantages of TeraSec and similar technologies compared with conventional security measures as well as threats to fundamental values and rights.



## (7) Selected Literature

### Security

- Commission on Human Security (2003): Human Security now, New York.
- The Human Security Center (2005): Human Security Report ([www.humansecurityreport.info](http://www.humansecurityreport.info)).
- Glaeßner, Gert-Joachim (2003): Sicherheit in Freiheit. Die Schutzfunktion des demokratischen Staates und die Freiheit der Bürger, Opladen: Leske+Budrich.
- Johnston, Les / Shearing, Clifford (2003): Governing Security. Explorations in policing and justice, London / New York: Routledge.
- Ramakrishnan, A.K. (2004): Conceptualising Security, in: Bhattacharya, Purusottam et al. (ed.): Anatomy of Fear, New Delhi: Lancer's Books, pp. 60-73.

### Freedom

- Berlin, Isaiah (1969): Four Essays on Liberty, Oxford: University Press.
- Frankfurt, Harry G. (1971): Freedom of the Will and the Concept of a Person, in: Journal of Philosophy, 68, pp. 5-20.
- Franklin, Benjamin (1964 [1755]): Pennsylvania Assembly: Reply to the Governor, November 11, 1755, in: Leonard W. Labaree, Leonard W. (ed.): The Papers of Benjamin Franklin, vol. 6.

### Justice

- Adey, Peter (2004): Secured and Sorted Mobilities: Examples from the Airport, in: Surveillance & Society, 1, 4, pp. 500-519 ([www.surveillance-and-society.org](http://www.surveillance-and-society.org)).
- Caney, Simon (2005): Justice Beyond Borders. A Global Political Theory, Oxford: University Press.
- Morgan, Nigel / Pritchard, Annette (2005): Security and social ,sorting'. Traversing the surveillance-tourism dialectic, in: tourist studies, 5, 2, pp. 115-132.
- Sen, Amartya (1992): Inequality Re-examined, Cambridge: Harvard University Press.

### Privacy

- Aas, Katja Franko (2006): 'The body does not lie': Identity, risk and trust in technoculture, in: Crime, Media, Culture, 2, 2, pp. 143-158.
- Bogard, William (1996): The simulation of surveillance. Hypercontrol in telematic societies, Cambridge: University Press.
- Dandekar, Natalie (1993): Privacy: An understanding for embodied persons, in: The Philosophical Forum, XXIV, 4 (summer), pp. 331-348.
- Dubbeld, Lynsey (2003): Observing bodies. Camera surveillance and the significance of the body, in: Ethics and Information Technology, 5, pp. 151-162.
- Ethics and Information Technology, Special Issue on Privacy and Data Privacy Protection in Asia, 7 (2005).
- Patton, Jason W. (2000): Protecting privacy in public? Surveillance technologies and the value of public places, in: Ethics and Information Technology, 2, pp. 181-187.