

## **The Security Principle – a Challenge to the Right of Privacy and of Freedom of Information**

Prof. Dr. Marie-Theres Tinnefeld, München (University of Applied Sciences)

Presented at the first annual European Freedom Summit, July 2, 2007 in Berlin

Translated from the German by Sean G. Penny

### **I. Introduction**

Terrorism and Security are topics of great importance after the terrorist attacks of 9/11. Since then, the United States has required more “predicative offense” by the USA PATRIOT Act. The number of these has expanded throughout the world to justify things such as wiretapping. Legal authorities in Europe are also more and more interested in “preventive” or “forefield” (from the German Vorfeld) surveillance even of the absolute core area of privacy. In the following, with the help of newspaper and magazine cartoons, several legal surveillance techniques will be described. In regard to the potential for controversy, these cartoons are a medium of free expression and a form of “legal design.” On the test stand the conflicts between security and democratic freedoms, especially the legality of privacy surveillance and the restrictive approach to freedom of information requests.

Preventive surveillance is different from its traditional use for investigating a specific criminal offense, which requires proof that a crime has taken place or is likely to occur. Preventive surveillance lacks any such connection to a specific criminal act (Albrecht et al. 2003: 440). The European Union, in a directive (ABIEG Nr. L 105 v. 13.4.2006, 37), by the governmental use of data mining techniques, explicitly permits the preventive surveillance of the noncontent, or telecommunications attributes: name, address, billing choices; e-mail addresses to which a message is sent; digital data, such as bank account numbers; datas of contact between patients and doctors or the press and their informants, etc. Noncontent data reveal much about the behavior of an individual, and are increasingly important to law enforcement officials. Under the

new national telecommunications acts security authorities and intelligence agencies of the European Union Member Nations have the authority for intervention, especially concerning preventive surveillance of telecommunications attributes, that telecommunication providers are required to retain for specified amount of time. In Germany they must do so for six months.

Widespread publicity has demonstrated the problem with the use of data mining, for example, in cases of the airport watchlist and the Transportation Security Administration. “The danger is that this activity will magnify problems that already exists with data errors, poor data integration (names recorded in different ways in different records) and data security (the danger that the personal data will be misappropriated or otherwise compromised.” As the New York Times reported: “There is no way to find out if you are on the list until you check in for a flight. Worse, there may be no way off.”

London and other capitals in Great Britain are installing extensive monitoring systems, primarily made up of Closed Circuit Television-Cameras (CCTV-Cameras). The New York Times International (November 3, 2006, A11) is concerned with the growing state and commercial intrusions into peoples' lives that ranked Britain among Russia and China as “endemic surveillance societies.” The “Anonymity of the City,” still something assumed in the last century, is not only giving way in England to “Round-the-Clock-Surveillance,” which prevents private and personal communication styles and habits, but it is to be expected that video surveillance, biometric identification methods, and RFID (Radio frequency identification) identification will soon become networked in a widespread manner, and the ability to compile profiles of the usage and movements of people will be available. Is ubiquitous and pervasive computing a means of offering security in the fight against terrorism?

Fundamentalist terrorism is unpredictable and assaults those who are defenseless. The mutual nature of attack and defense is abolished. Terrorism wants to instill panic, but as the concerned

states intensify safety measures with anti-terrorism laws, these laws at the same time restrict the freedom of those protected. A further problem is the American concept of a “war on terror” which encourages governments to attack “rogue states.” This idea faces not only the use of weapons but also a forfield surveillance of people. The use of anti-terrorism techniques raises new privacy threats. The USA government is making a significant effort to track the movements and activities of Americans, keeping extensive files even of foreigners, for example air passengers. There is too an inclination to secrecy, a restrictive approach to freedom of information (Cheney v. U.S. Dist. Court for D.C, 124 S. Ct. 2576, 2004).

Action that impinges upon civil liberties are likely to last for decades and might change the nature of an open and free society. One should not accept an approach that is similar to the “black hole” theory of constitutional rights in wartime. Under this approach “constitutionally guaranteed civil liberties disappear into a “black-hole” during war, only to reemerge once the nation is on peace.” Democratic liberties cannot merely be pushed aside until the threat from terrorism abates. The question is to recognize the difficult conflict between security and democratic freedoms. To balance the two is the art of a policy that deserves to be called fair, just, and wise.

## **II. The Right of Privacy in a Security and Prevention State**

Neither freedom of information, nor the protection of privacy are the guidelines of the European Union and its member states, but rather it is security - at all times and in all places. The redrafting of a government policy of guaranteed security into a comprehensive “Basic Right of Security” should justify the restriction of individual freedoms, even of those citizens who have no criminal record. That the free development of identity and the guarantee of an intact intimacy and privacy are part of a liberal constitutional state, seem to have been lost in the eyes of the citizens and of the politicians

The state's understanding of the fear-based connection between promises of security and oppression is shrinking, at least in the sense of the political theory of Hobbes. Instead of using words, this change can be better expressed with the title picture of the English first edition of Thomas Hobbes's "Leviathan" (London 1651), a book that arose from the English civil war during the 1700s. The visually powerful Leviathan (the name of a biblical sea monster in Isaiah 27, 1; Job 41, 24, 26), appears as a strong, authoritarian sovereign (Bredenkamp 1999: 266). Its cells are those humans who have contractually transferred their rights of power to the state in exchange for protection and security, thereby creating a single, monopolized power. The fusing of these subjects onto the body of the giant corresponds to the "uno actu" realized construction of the contract, which allows of no other perspective

This having been said, security today, for the most part, no longer means the certainty of legal freedom of a citizen against arbitrary state interference, but instead means never ending activity by the state for the protection of the citizen. With the connection being made between internal and external security, and with the shifting of the idea of safety away from the "certainty of legal freedom" to one of limitless risk prevention, the modern prevention state shows its full form (Denninger 2005: 227). The exposure of privacy becomes as self-evident "as traffic lights and fire hydrants" (Raban 2005: 6).

This opinion raises significant constitutional questions. The German Federal Constitutional Court (Bundesverfassungsgericht) has consistently emphasized that the constitution recognizes "a last inviolable sphere of privacy, into which the public force is simply not allowed." Even serious interests of the general public cannot warrant governmental intervention into this sphere; a consideration in accordance with the principle of proportionality is not permissible, if the absolute core area of privacy is concerned (BVerfGE 80, 367, 373; BVerfGE 109, 278, 357 – Eavesdropping).

The “Great Eavesdropping Offensive Decision” of the Constitutional Court in 2004 brings into question special aspects of the legal regulation of telecommunications surveillance in Germany. Part of this decision rests on the important role that one's home and its physical space plays in ensuring a “right to be left alone.” The home “is, a last refuge, a means of safeguarding human dignity” (BVerfGE 109, 279, 314). How, if at all, can a measure by the security authorities be legally arranged into the criminal code, without the core area of privacy being touched? This question arises at present regarding the secret online searching of the personal PC of a suspect. The German Federal Court (Bundesgerichtshof) forbid such searching on February 7, 2007, due to the present legal situation concerning a serious infringement of information privacy (Tinnefeld 2007: 137f.). The data stored on the computer (ideas, E-mails, documents, diaries, love letters, family photos) belong to the right of privacy, to a concretely recognized sphere of “human dignity,” that should be protected by the rule of law.

The right of privacy, in its various characteristics, is protected in the European Human Rights Convention (Article 8 EHRC) and in the German Constitution (informal self-destination/informal privacy - Articles 2 I /Art. 1 I GG; protection of telecommunications secrecy – Article 10 GG; the respect for the home – Article 13 GG). In Germany, constitutional safeguards remain in place unless all parties to a communication offer their consent to telecommunications surveillance. Communicative fundamental rights depend upon the protection of privacy. In order to make free and informed decisions, there is a fundamental need to protect the freedom of thought and conscience in particular, as well as free speech, and freedom of information (Article 9 and Article 10 EHRC; Article 4 and 5 GG).

Since the time of the French Enlightenment and in the name of the ultimate Enlightenment value “tolerance,” freedom of speech was the central basic right of the USA: “Exposure of the self to others in varying degrees is a commitment of life in a civilized community. The risk of this

exposure is an essential incident of life in a society which places a primary value on freedom of speech and press” (Time, Inc. v. Hill, 385 U.S. 374, 388 (1967)).

Tolerance is an essential element of a free society. But also in addition it is necessary to keep in check those forces that threaten these core values, no matter from where there are coming; whether from security fanatics on one side or from Islamic fundamentalist who disseminate terror on the other. Tolerance as well as freedom must be in proportion to the necessary requirements of a free society that at the same time understands its obligation to protect itself.

“The mighty woman with a torch,” at the entrance of the port of New York, symbolizes what was up until now the guiding value of the USA as “Liberty enlightening the World,” a notion deeply seated as freedoms of opinion and of the press in the First Amendment of the American Constitution: “Congress shall make no law [...] abridging the freedom of speech and the press.” The Bush administration currently has a very restrictive approach to civil liberties, especially with regards to free speech and freedom of information. The former Attorney General Attorney merits special criticism about certain controversial decisions. These include the reducing of protection from FBI surveillance of religious and political meetings, and easing the conditions under which FBI agents can carry out Internet research of individuals.

That each uncovered plot to commit crime is preferable to an additional successful search must not be specially discussed. Even in this respect, the prevention state can allege its fundamental obligations of protection, if it is a matter of legally protected property such as life and health, in whose interest it [the state] acts in the war on terror, for example. But the greater a danger is or the greater it furthers the citizens' fear of crime, through a visualization of terror produced by the mass media the more preventive restrictions of freedom appear to be appropriate. One must be familiar with this face of the prevention state, if he wishes to set down a judicious and reasonable security measure that restricts freedom.

Computer surveillance, covert observers, secret hacking of private computers, the mass storage of telecommunications attributes; all these things are at the forefront of what was up until now the inalienable, constitutional “Reasonable Suspicion” and are some of the keywords which signal the end of the traditional liberal legal security. But beyond the reach of the law are political security-prevention programs, which address the concept of predicate, personal profiling. Scotland Yard, for example, is working on a database of future murderers. With it, people who are labeled as possible offenders, because of their psychological profiles, can be arrested for precautionary reasons, based upon information from former romantic partners and mental health services. In the field of criminal law, scientists are in support of preventive mass screening of all juveniles, in order to detect whether they might later develop aggressive or criminal qualities. Whereas biometric cameras used for facial-recognition (i.e., at the Hauptbahnhof in Mainz) more or less end at a person's forehead, there are attempts to “x-ray” the highly complex human brain, with the intention of finding out about what goes on behind the forehead. The question of Neuroscreenings also belongs here - that is, the question of a comprehensive examination of criminal predispositions regarded as neurological defects.

With a neuroscreening method for preventive purposes, for instance a brain scan at the airport, the path towards an “all-knowing” prevention state begins to reveal itself. The constitution, however, should not only keep the people from such an “Atlantis” of universal internal and external security. Citizens themselves should be afraid of a life united with such a security mentality. It is a mentality that the masterminds of the terrorist networks are presently watching. What sort of life do people exchange for that impact? Steven Spielberg's Science-Fiction *Minority- Report* (2002) acts as writing on the wall.

### **III. The Right of Privacy, the Minority Report, and Guantanamo**

The film *Minority Report* portrays a country in which there exist no crime and allegedly absolute security. In the capital of the USA in the Year 2054 one finds surveillance cameras in every public place, which identify each person with an eye-scan. During criminal investigations in the film, mobile surveillance robots, so-called Spyderys (a term coined from the combination of Spy and Spider), are used. Anyone who tries to evade their retinal scan is stunned with an electric shock and arrested.

The security authorities (Pre-Crime) seek out and arrest those potential offenders who are profiled by the so-called Pre-Cogs. The limitless and immeasurable nature of the prevention plan has immediate practical effects/impacts on the way information is shared in the country, with all abnormal predictions kept secret in the *Minority Report* of the primary Pre-Cog. People who are known to be innocent nevertheless disappear in cages. The individual is no longer a subject of concern, but is instead replaced with the “State Security Policy.” For these reasons neither the recognition of human dignity, nor the prohibition of torture, and neither the right to a privacy worthy of being protected, nor an intact home free of monitoring, stand a chance. It is not a coincidence if this entire picture reminds us of the torture prisons in Abu Ghraib and Guantánamo that the USA set up against terrorism and which were, in the case of Murat Kurnaz, partially supported by Europe. All this has taken place even though three systems of legal rights applied to these locations: the human rights laws of the UNO, the international humanitarian laws, and the Constitution of the United States with its guarantees of Habeas-Corpus and “due process.” One can conclude from the due process clause of the 14<sup>th</sup> amendment a constitutionally protected reasonable right of privacy in front of infringements by the state (*Katz v. United States*, 389 U.S. 347, 350, 1967).

Like the USA, European states have also ratified the UNO-Agreement on Civil Rights of 1966,

whereby no one may “be subjected to torture or cruel, inhumane, or demeaning treatment or punishment” (Article 7). All ratifying states are themselves responsible for the adherence to this agreement, as well as the concerns of what goes on outside their own territories.

The concept of Guantanamo threatens human rights and the core values of a democratic society. As noted above freedom of information is one of the basis rights of a citizen. The “peoples’ right to know” is covered by the American Freedom of Information Act (FOIA), and by several newly established Freedom of Information Laws in the European Union.

#### **IV. Closing/Final Remarks**

In the Prevention state, the legal philosophy of “if in doubt choose freedom” is replaced with the motto “if in doubt choose security.” But is absolute security possible? Will security become thought of as a condition in which the “worry” and the fear that we blindly strike at with fists blaring, can be eliminated with an immeasurable and limitless preventive or forfield surveillance? Goethe's Faust II (Act V) remains today, not least of all, an important literary moment, because it exposes this paradox. The problem that it shows us at the beginning of the third millennium has grown in severity because of the terrorist networks.

The Minority Report shows that self-determined lifestyle and open communication become lost under the pressure of preventive surveillance, the dangers of which are already present and should be stifled while they are still nascent. The normal legal procedures have been discarded. Should states be allowed to claim a “legal black hole,” in order to have a free hand in the fight against terrorism? As noted above, terrorism, in its various forms, does not pose a temporary threat. Should the security paradigm, however, be declared as a normal procedure of government? The offending cartoons try to visualize the “legal design” of this situation.

Democratic liberties cannot be pushed aside until the threat from terrorism abates. It is a legal

obligation to inform those persons placed under surveillance afterwards. The German Federal Constitutional Court handed down this decision in “Great Eavesdropping Offensive,” which emphasized the fundamental nature of the right of an individual to be informed, that he or she had been placed under surveillance. Ultimately, it is necessary to evaluate the impact of preventive surveillance on the outcome of criminal prosecution and of the acts of terror.