"Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe"

Project acronym: **SurPRISE**

Collaborative Project

Grant Agreement No.: 285492

FP7 Call Topic: SEC-2011.6.5-2: The Relationship Between Human Privacy And Security

Start of project: February 2012

Duration: 36 Months

D 3.1 – Report on surveillance technology and privacy enhancing design

Lead Beneficiary: ULD

Author(s): Eva Schlehahn (ULD), Marit Hansen (ULD), Jaro Sterbik-Lamina (ITA/OEAW, for chapter 2.2.3, Smart Meter Surveillance), Javier Sempere Samaniego (formerly APDCM, for chapter 2.3.2, Body scanners)

Due Date: January 2013

Submission Date: June 2013

Dissemination Level: Public

Version: 1

This document was developed by the SurPRISE project (http://www.surprise-project.eu), co-funded within the Seventh Framework Program (FP7). SurPRISE re-examines the relationship between security and privacy. SurPRISE will provide new insights into the relation between surveillance, privacy and security, taking into account the European citizens' perspective as a central element. It will also explore options for less privacy infringing security technologies and for non-surveillance oriented security solutions, aiming at better informed debates of security policies.

The SurPRISE project is conducted by a consortium consisting of the following partners:

Institut für Technikfolgen-Abschätzung / Oesterreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM	
Instituto de Politicas y Bienes Publicos/ Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	CSIC	
Teknologirådet - The Danish Board of Technology Foundation, Denmark	DBT	
European University Institute, Italy	EUI	
Verein für Rechts-und Kriminalsoziologie, Austria	IRKS	
Median Opinion and Market Research Limited Company, Hungary	Median	
Teknologirådet - The Norwegian Board of Technology, Norway	NBT	
The Open University, United Kingdom	OU	
TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland	TA-SWISS	
Unabhängiges Landeszentrum für Datenschutz, Germany	ULD	

*APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Table of Contents

List of Abbreviations

Abbreviation	Meaning
2D	Two-dimensional
2G	Second generation
3D	Three-dimensional
3G	Third generation
4D	Four-dimensional
API	Advanced Passenger Information System
ATM	Automated Teller Machine
AuC	Authentication Centre
C/A	Coarse Acquisition
CCC	Chaos Computer Club
CCTV	Closed Circuit Television
CORS	Continuously Operating Reference Stations
DDOS	Distributed Denial-of-Service
DNA	Deoxyribonucleic Acid
DNS	Domain Name System
DPI	Deep Packet Inspection
DSO	Distribution Service Operator
DSS	Digital Slow Shuttering
DVR	Digital Video Recorder
EIR	Equipment Identity Register
esa	European Space Agency
ETSI	European Telecommunications Standards Institute
EU	European Union
FAA	Federal Aviation Administration (of the United States of America)
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HLR	Home Location Register
HTTP	Hypertext Transfer Protocol
ID	Identifier, Identification Number
IdM	Identity Management
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IR	Infrared
ISCORS	Interagency Steering Committee on Radiation Standards
ISP	Internet Service Provider
LAN	Local Area Network
LBS	Location-Based Service
MSC	Mobile Switching Centre

NALM	Nonintrusive Appliance Load Monitoring
NGO	Non-Governmental Organisation
NPO	Non-Profit Organisation
NTRIP	Networked Transport of RTCM via Internet Protocol
NTSC	National Television System Committee
OSI	Open Systems Interconnection
PAL	Phase Alternating Line
PbD	Privacy by Design
PC	Personal Computer
PET	Privacy-Enhancing Technology
PNR	Passenger Name Record
POS	Point of Sale
PRN	Pseudo-Random Number
PTZ	Pan-Tilt-Zoom
RF	Radio Frequency
RPAS	Remotely Piloted Aircraft System
RTCM	Radio Technical Commission for Maritime Services
SbD	Security by Design
SIM	Subscriber Identification Module
SMS	Short Message Service
SOSS	Surveillance-Oriented Security Solutions
SOST	Surveillance-Oriented Security Technologies
SPI	Shallow Packet Inspection
SQL	Structured Query Language
SVGA	Super Video Graphics Array
SXGA	Super Extended Graphics Array
TCP	Transmission Control Protocol
TSMI	Temporary Mobile Subscriber Identity
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UK	United Kingdom
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
U.S.	United States of America
VGA	Video Graphics Array
VLR	Visitor Location Register
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network
WAAS	Wide Area Augmentation System
WLAN	Wireless Local Area Network
XML	Extensible Markup Language

Executive Summary

This deliverable reviews the current state of the art regarding existent and emerging surveillance-oriented security technologies (hereafter referred to as SOSTs). So within the context of surveillance-oriented security solutions (hereafter referred to as SOSSs), this deliverable focuses mainly on selected technological solutions which are proposed as answers to security issues in the European Union (EU). Since these SOSTs are often seen as having negative impact on privacy and other civil rights issues of European citizens, it is crucial to closely assess and evaluate such technologies to support responsible governmental institutions on a national as well as on a European level. To provide a well-researched basis for such an assessment, we have selected a number of SOSTs to describe their functionality and effectiveness from a technological point of view. Since a description of the full range of all existent SOSTs is not possible within the scope of the SurPRISE project, we tried to select technologies which we found have a great impact on the lives of European citizens nowadays and will continue to have a great impact in the foreseeable future. These selected technologies are categorized into different sections for a clearer structure. These sections are:

- Public space surveillance
  - Smart CCTV
  - Drones
- Network & targeted device surveillance
  - Deep Packet Inspection for Internet surveillance
  - Content surveillance on targeted devices
- Biometrics & body scanners
  - Facial recognition
  - Body scanners

Since the use of many security-related technologies provides inherent privacy and other civil rights issues for citizens, we have striven to include technologies which have not yet been viewed in-depth from a privacy angle. Owing to this fact, we explored for each technology the possibility of implementing the Privacy by Design concept to maintain lawfulness and ethical deployment. While reviewing the current state of the art of the aforementioned technologies, we found that some surveillance-oriented security technologies appear unacceptable due to their intrusive and even repressive nature, making an earnest assessment of the desired security enhancement necessary, taking into account the principles and ideals of a democratic Europe.

In Smart CCTV (Closed Circuit Television), a significantly more comprehensive surveillance of citizens in public space areas is conducted, involving advanced features of the technology such as face & motion detection, crowd & directional flow detection, unattended or missing object detection, facial recognition, license plate recognition, targeting/positioning/tracking of subjects and objects, behavioural pattern & anomaly recognition, image quality & camera zooming enhancement, audio recording, and additional data matching & analytics capabilities. Drawbacks for the merely technical effectiveness have been especially found in lack of adaptive systems as well as necessary prerequisites for camera positioning, lighting and other conditions to produce adequate image qualities. Beyond the question of faultlessness of the technology, Smart CCTV has repeatedly been doubted as being an adequate measure to reduce crime in public spaces. Moreover, the Smart CCTV has some impact on human rights matters especially with regard to behavioural pattern recognition enhancement since enabling algorithms still depend on humanly controlled and stereotypical pre-definition of what is to be considered “normal” and “abnormal”, significantly increasing the risk of discriminatory assessment of human behaviour. Potential Privacy by Design approaches like the exclusion of certain areas (no insight to private property through doors/windows), exclusion of audio recording, a recording limited to alarm-triggered events, de-identification of individuals (pixelating, blurring, obfuscating, masking), protection of recordings via encryption etc., access controls, and deletion routines may be of help to reduce the impact of this measure.

Drones (Unmanned Aerial Vehicles – UAV) are besides Smart CCTV a technical approach to conduct the surveillance of public spaces for the purpose of enhancing security. Varying greatly in size, flying abilities and equipment, drones may be deployed for a multitude of purposes and be equipped with varying flying abilities. Additional equipment may also provide for a diversified spectrum of possibilities, for example through an extension of the UAV system by Smart CCTV, sensors, panoptic equipment, radars, Wi-Fi and other communications interception technology, chemical or radiation detection, and armoury. Despite already being used widely, crashes are still very common, mostly due to latency issues, inconvenient weather conditions, loss or disruption of data & communication links, faults or malfunctions of the machine components, human error factors. Drones are also still prone to hacking attempts, the ones merely reliant on GPS (Global Positioning System) positioning having proven especially vulnerable. Beyond these technical weaknesses, drones also come along with severe concerns regarding privacy and other human rights. Not only freedom of expression and association issues arises when they are used in public, for example at demonstrations, but they might also endanger the inviolability of the home of citizens by giving insight to windows, and of gardens and backyards. Whereas it must be seen how much can be achieved by deploying Privacy by Design in the advanced equipment, such approaches for the UAVs have not yet come far.

In the context of network surveillance, we described Deep Packet Inspection (DPI) for Internet surveillance as one possibility to monitor data and traffic on the Internet, conducted through the Internet Service Providers. DPI inspects data packets arriving at and leaving from a device, thereby inspecting all seven layers of the data packets. By doing so, it recognises varying information contained in headers and payload of each data packets, such as protocols, applications, URLs (Uniform Resource Locators, in particular web site addresses), media content (specific instances of recorded music, movies, images or books), text strings, and data with a specific format (e. g., credit card numbers, Social Security Numbers) and more. Thus, this technology is well equipped to learn the content of the communication between many users. There is little to no reliable data how effective Internet surveillance technologies are really with regard to preventing and investigating criminal activities on the Internet. Moreover, appropriate Privacy by Design approaches are yet severely lacking in this field of technology. Thus we found that DPI technology being able to monitor, filter, analyse, store away and manipulate all kinds of digital citizen data has high potential to be misused for social discrimination, political repression, censorship and serious infringement on sensitive areas of private life.

The infiltration of a specifically targeted device, in contrast to wide-scoped Internet surveillance with the help of DPI, occurs through software (code) which was brought onto the personal system. Often, Trojan Horses brought onto the individual devices (creating a backdoor to the system) open up the possibility of intercepting Internet telecommunications before or after encryption for the data transmission. This software functions covertly, without revealing its real functionalities to the user of the device. Also, beyond the mere interception of telecommunication, the code brought onto the device this way possibly enables further means of surveillance, for example by being accompanied by additional malware. This malware may facilitate further surveillance as well as influence on the system, for example by monitoring the system, DPI, key logging, screenshots, filtering, country tracking, execution of programs & processes, access to cameras and microphones, manipulation of data, and inducing system crashes. Inbuilt update functions of such surveillance systems enable practically limitless possibilities, making Privacy by Design approaches very difficult to achieve.

Smart meter surveillance is aimed at energy metering devices in households. The collected data on the consumption of electrical energy may under circumstances enable the surveillance of the citizen's everyday life, including life conditions and habits of a person, whereas some Privacy by Design approaches already exist. In the section for location trackers, we focused on mobile device tracking of individuals. Most real-time location systems nowadays are elements of built-in mobile wireless systems. The functions provided may range from routing incoming or outgoing calls, accurate geo-locating, navigation and timing. We have focused on means to obtain the location by GPS positioning, cell tower records for mobile phone location data, and Silent SMS (Short Message Service) for mobile phone

location data. This repeatedly collected or requested location data, even in anonymised or pseudonymised form, may reveal information about frequently visited places, enable predictions about future whereabouts, determination of means of transportation (by foot, car etc., how fast is the person moving?), allow an assessment of likely living or work places, and last but not least make the identification of the individual possible. The positioning, location and tracking of mobile devices may be prevented or circumvented by using different techniques. But these come along with significant disadvantages and dangers. So such broad measures mostly concern data of innocent citizens being put under general suspicion. Due to the above-described nature of the communication, navigation and timing services being offered by the respective network providers, the collection and processing of personal data seems very difficult to avoid. Until on-going research in terms of Privacy by Design has achieved a sufficient level of efficiency and deployment, any privacy-preserving approaches in this field will at the time being mostly entail organisational measures to restrict access to the data bases.

Beyond the network and targeted device surveillance, we finally had a closer look at biometrics as well as body scanners. Facial recognition is one of the biometric techniques being used in a multitude of areas already and also still being subjected to intensive research with regard to further application fields. Starting point is the measurement of the bodily characteristic or trait to provide a biometric sample, which is then used to create a template file. Then, this template may be used for several possible purposes, such as matching it with a comparison image. The typical model of such a measurement process encompasses three different stages, which are enrolment, template creation, and matching. Due to weaknesses of two-dimensional (2D) facial recognition systems, research & development efforts of the last years have concentrated on the development of three-dimensional (3D) recognition processes taking into account the three-dimensional condition of the human face. So far, these efforts still provide for yet unsatisfying results. Mostly, it can be said that the capture, evaluation, and comparison of biometric characteristics and traits may be under circumstances faulty due to measurement errors, caused by influential factors such as aging, beards, glasses & contact lenses, make up, facial expression, and light settings during capture. One very crucial concern regarding facial recognition technologies is function creep: in other words, the inherent potential of exceeding data collection beyond the originally intended scope by the digital capture of the biometric traits. The facial physiognomy allows for conclusions regarding age, gender, ethnical origin, or even health status of the person. Moreover, the creation of unalterable and unique digital biometric reference set makes it ideal connection or linking point for any kind of enrichment with data from other sources for profiling. For facial recognition, a number of Privacy by Design approaches have been endorsed by experts, and research is still seeking to find and improve means of preventing unauthorised secondary uses, loss, or misuse.

Body scanners are a fairly new technology believed by experts able to guarantee security in a more efficient way than traditional methods to secure e. g. aviation. This is believed to be so due to the fact that the new-generation body scanners would be able to accurately detect liquids and non-metallic objects. The most commonly used body scanners techniques are passive millimetre waves, active millimetre waves, X-ray backscatter, and X-ray transmission imagery. Due to the high doses of radiation emitted by X-ray transmission imagery and inherent health matters, no use of this technology is foreseen in Europe. Some tests and studies presented differing results regarding the effectiveness of body scanners, but revealed a generally high rate of false alarms. Beyond the effectiveness and health issues, body scanners were also criticised due to their negative on human rights, especially with regard to human dignity, privacy and data protection. Privacy by Design approaches are yet few and in between, but first steps have been taken, such as by recording & storage limitations, access controls, encryption and system audits.

Note that the chosen technologies described in this text by no means cover the full landscape. Instead, they have very different properties which exemplify the variety in the field: For instance, surveillance technologies such as Smart CCTV is to be found in professional, but also private settings; drones are positioned in the range between military instruments and toys for everybody; the analysis of technically available data can be done via Deep Packet Inspection for multiple purposes and usually covers all

communication available whereas online investigation is targeted to specific individuals; facial recognition gets further importance because the algorithms are meanwhile even part of social networks such as Facebook or Google+; body scanner technologies are debated not only because of their questionable efficiency, but also because meanwhile privacy-respecting solutions become available on the market.

After the technology descriptions, we included a short chapter addressing new means of data matching, linkage and analysis to explore the further consequences these have by being linked to the previously described technologies. Finally, we conclude with the observation that a more contextual view of these technologies is needed to assess their implications for civil rights, especially taking into account emerging possibilities for broader data linkage and profiling.

Privacy by Design as a concept as well as a guideline for specific measures to be taken often appears insufficient, dependent on which technology is in question. This is due to the fact that some SOSTs have an inherently intrusive nature, which makes it very difficult to implement Privacy by Design measures. Moreover, we find that more research in this field is sorely needed. Whenever surveillance-oriented security technologies appear unacceptable owing to their intrusive and even repressive nature, we propose to earnestly assess the desired security enhancement and balance it against the principles and ideals of a democratic Europe which is governed in a transparent, ethical and citizen-friendly manner. Hopefully, with the creation of this document, we have shaped a set of technology descriptions which can be used to evaluate those surveillance-oriented security technologies with regard to the aforementioned principles and ideals and acquire possible acceptability criteria within the SurPRISE project.

Objectives

This deliverable D3.1 was created for the European FP7-funded project SurPRISE. The project acronym stands for 'Surveillance, Privacy and Security: A large-scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe'. Within this project, D3.1 is part of Work Package 3 (called 'Exploring the Challenges'), which is focused on identifying the main challenges and possible resolutions in the context of the current technical, societal, legal and political state of the art regarding security and privacy in Europe as well as emerging developments. Thereby, the findings of the first year of research in WP3 will be presented in three main documents, which are the deliverables D3.1 (report on surveillance technology and privacy-enhancing design), D3.2 (report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy), and D3.3 (report on security-enhancing options that are not based on surveillance technologies). D3.2 focuses mainly on the state of the art and current as well as emerging challenges and options related to privacy and security in the European Union from political and legal viewpoint. Reviewing recent judgements and legislation linked to privacy as well as to surveillance-oriented security solutions and technologies (SOSSs and SOSTs), it derives objectives related to the fundamental norm to privacy, legal permissibility of infringements and a reflection upon European judgements balancing out issues of security against those of privacy. D3.3 focuses on societal developments related to security and reviews non-technological alternatives. These alternatives, entailing theories, concepts and methods are then evaluated with regard to their potential to providing real opportunities compared to technological solutions. So the outcome of this analysis is not to be seen as a stand-alone, but will serve as input for the other sub-tasks of WP3.

D3.1 contributes to the assessment regarding the question whether security as a legitimate goal of society may be achieved and maintained while still adequately taking into account the civil rights of European citizens, especially with regard to privacy intrusions. In doing so, WP3 aids in identifying key challenges of security SOSTs with regard to privacy and other fundamental rights. The results will also be relevant for other work packages in the project, namely WP2 (framing the assessment), WP4 (questionnaire and information material) and WP6 (analysis and synthesis). Moreover, they will support the planning of a large-scale citizen consultation to be conducted within the SurPRISE project by giving input on security solutions as example use cases to be presented to the citizens participating. Hence, the results of this document will serve as presentation and discussion material for the project-initiated citizen consultation and in stakeholder and user workshops during the further project runtime (this tackles the WPs 5-7). Finally, the three deliverables of WP3 will form the foundation of a synthesis report also to be conducted in this work package (D3.4), which presents a broader context for the individual results. Ultimately, this document aims at feeding into the general goal of SurPRISE, which is shaping lawful and ethical guiding principles finding a better suited balance between privacy and security issues in the European Union than the classical privacy-security trade-off model.

1 Methodology and concepts

As a sub part of work package WP3 in the SurPRISE project, task WP3.1 encompasses the identification and description of current and emerging surveillance technologies. In doing so, we aim at providing a consistent research approach among the work packages of the project. Owing to this intention, we lay the foundation to the work of this document by using a basic joint definition of the term 'surveillance'. This offers the reader of this document a hopefully comprehensive understanding of governmental surveillance dedicated to serving security purposes. So, we define surveillance as *'the targeted or systematic monitoring, by governmental organizations and their partners, of persons, places, items, infrastructures or flows of information, in order to identify hazards and manage risk and to enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future. We are stating, furthermore, that the major aim of surveillance is to name, identify, monitor and track individuals and their actions.'*[1]

However, a comprehensive description of all existent surveillance technologies is far beyond the reach of this document. Therefore, we concentrate on fairly new technologies or technology developments which pose interesting legal and ethical challenges from a privacy perspective. In doing so, we will for each described technology follow in general the same structure: First, we will introduce the technical capabilities of the technology itself, in its standard and in its advanced forms. Then, we will briefly assess the effectiveness of the measure in question from a purely functional and technological point of view and not from the impact on security. In this context, we may per technology also highlight the most evident risks to security, for example by weaknesses or faults of the technology itself. In the light of the previous findings, we will then briefly assess the civil rights impact of said technology and potentially available and applicable Privacy by Design (PbD) approaches. On this account, we explicitly highlight that in the following, we will not elaborate comprehensively on all existing concepts of Privacy by Design and the related dogmatic debates. Rather, we would like to present some few concepts to enable the reader grasping the idea and goal of PbD in general: To counter the inherent dangers of surveillance technologies in relation to privacy and human rights matters, it is important to eliminate or at least minimise negative effects on citizens in balance with the desired security enhancement. Potential relief especially regarding the data protection and privacy issues, but also with positive effect on other civil liberties, might be provided by the PbD approach.

Since the 1990s the PbD approach has been strongly promoted by the Canadian Information & Privacy Commissioner Ann Cavoukian and others. It is a concept foreseeing that IT processes with their whole infrastructure and system as well as business and organisational processes should be designed with consideration of privacy issues right from the start, entailing the following core principles:

- Enabling privacy should be proactive, not reactive;
  privacy should be preventive, not remedial
- Privacy should be implemented as the default setting
- Privacy should be embedded into the design of the service/product from the very beginning
- Accommodation of all legitimate interests/objectives (positive-sum, not zero-sum)
- End-to-end security – full lifecycle protection of personal data

[1] Cf. D3.3 of the SurPRISE project (Report on security enhancing options that are not based on surveillance technologies), Chapter 2.2 "Security, surveillance and privacy as terms and concepts"

- Visibility and transparency should keep component parts and operations open to independent verification and forensics
- Respect for user privacy by offering knowledge and control[2]

To present the reader a small glimpse on the conceptual debates evolving around PbD and its relationship to security since then, we point to an alternative approach developed by the National IT and Telecom Agency in Copenhagen, Denmark, focusing on Security-by-Design (SbD) measures. This means that any kind of IT service should be designed with an architecture enabling minimal data disclosure.[3] This requirement can also apply to governmental surveillance contexts, since specifically in such cases there is a strong necessity of protecting citizens' fundamental rights aligned with the principles of the democratic order in the European member states. Still, there are some significant differences between Privacy by Design and Security. However, as mentioned before, we won't elaborate on these conceptual debates and rather focus on specific measures per technology which serve the interests of European citizens. This is to equip the reader not with merely theoretical discussion ground, but rather with solid and directly applicable resolution possibilities in each field of technology. Thereby, we point out that both aforementioned approaches definitely have in common the orientation towards higher data protection standards.[4] In the light of these goals, we will present technical solutions compatible with or at least inspired by these concepts as far as existent and applicable. Where appropriate and fitting into the technical context, we will also mention not only technical solutions, but complementing organisational solutions compliant with the idea of Privacy by Design. To finally be able to draw conclusions, we thereby explore whether the individual technologies may be suitable to be deployed in a manner respecting fundamental rights of European citizens.

To empower the reader in terms of easier orientation, we classified the selected technologies into four sections, which are:

- Public space surveillance
- Network & targeted device surveillance
- Biometrics & body scanners
- Data matching, linkage & analysis

Starting with methods of public space surveillance, we will introduce the recent developments in the field of CCTV. Since the conventional forms of CCTV in public spaces to enhance security are well known and documented, innovative possibilities of advanced equipment shape a whole new dimension of surveilling European citizens. Going from the visual forms of surveillance and taking into account more sophisticated paths of public space observation, we also describe drones as another method of surveillance in this context. The next section provides descriptions of technologies in close relation to the personal devices of citizens to be surveilled. This may concern devices such as personal computers (PCs), laptops, smartphones, navigation systems and smart meters. At the same time, we shed light onto network surveillance. Therefore, this section will provide descriptions in the field of the following areas: Deep Packet Inspection for Internet surveillance, content surveillance on targeted devices by Trojans, smart meter surveillance, and location trackers. Then we present a chapter about biometrics in the form of facial recognition as well as about body scanners as a surveillance tool conducting a physical analysis of an individual's body. All of these aforementioned technologies come with beneficial security-

[2] Ann Cavoukian, Information & Privacy Commissioner Ontario, Canada, "Privacy by Design – The 7 Foundational Principles", originally published: August 2009, latest revision December 2012: "Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices" for a further overview of the initial concept, see http://www.privacybydesign.ca/

[3] The National IT and Telecom Agency, Copenhagen, Denmark: New Digital Security Models – Discussion Paper, February 2011, pp. 11 ff.

[4] Cf. Ann Cavoukian, Martin E. Abrams, Scott Taylor, "Privacy by Design: Essential for Organizational Accountability and Strong Business Practices", pp. 8 ff.

enhancing capabilities as well as negative effects on the civil rights of European citizens. So, to convey a broader view of the influence that these technologies have on the everyday lives of European citizens, we set their deployment into context to the scope and impact of the collection, processing and storage of the data. To achieve this, we briefly introduce current and emerging means of data linkage, storage and analysis by methods of behavioural pattern and anomaly recognition as well as major data and profiling issues that are manifesting themselves independently from the prior mentioned technologies. Finally, we conclude with our findings about the technological developments of the modern world in the field of security and our assessment of their consequences for the average European citizen.

2 Surveillance technologies

Within the European Union, key global challenges related to security have moved more and more into the focus of policymakers. Interstate commerce and investment, ground-breaking innovations in the field of technology and political developments have shaped a different world view for many European citizens. While security is a precondition for prosperity and freedom, the means to achieve it are subject to intense discussions involving not only experts, but also the broader public. Technology can play a role in enhancing security in the most various fields. But often, such technologies may also have the potential to be misused for unauthorised governmental intrusion into the lives of innocent citizens, often covertly and without supervision. This potential is also often only apparent to those who have well-founded technical expertise. Since the rise of the modern digital world, citizens using the vast opportunities offered by online services mostly do not realise that these are prone to leaving traces of personal data, allowing a more comprehensive insight into their private lives. Moreover, the digital era brings forth new possibilities for using technologies where one cannot tell yet what impact these will have on our everyday lives. Some of these technologies even kindle concerns about basic principles of ethics, rousing issues about priorities to be set in the fields of civilian protection, privacy, freedom, and humanity.[5] Consequently, potentially negative effects of some technological approaches for enhancing security have already been discussed in some European research projects[6], and yet many complexities of the technologies remain obscure.

Within this document, we focus mainly on aspects of security which are related to terrorism and crime, thereby exploring the capabilities of existent and emerging surveillance-oriented security technologies (SOSTs). The technologies we focus on in this context are:

- Public space surveillance
  - Smart CCTV
  - Drones
- Network & targeted device surveillance
  - Deep Packet Inspection for Internet surveillance
  - Content surveillance on targeted devices
- Biometrics & body scanners
  - Facial recognition
  - Body scanners

We identified these technologies as having a significant impact on civil rights today as well as in the foreseeable future, thus their description will hopefully serve as a useful basis for assessing their impact and acceptability.

2.1 Public space surveillance

The surveillance of public places is mostly perceived by citizens as being monitored while situated in spaces open to the public, and thus comes with a Janus face. On the one hand, surveillance is seen as a measure of prevention and protection against security threats likely to happen in public spaces such as

---

[5] For example, this is the main focus of the Human Rights Watch report "Losing Humanity" tackling issues related to the use of drones, November 19th 2012, http://www.hrw.org/reports/2012/11/19/losing-humanity; also, these are issues seen as relevant in the digital sphere, see e. g. the multidisciplinary analysis published by Johannes Buchmann for acatech, Deutsche Akademie der Technikwissenschaften (German Academy for Technology Sciences), "Internet Privacy", September 2012, http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Projektberichte/acatech_STUDIE_Internet_Privacy_WEB.pdf

[6] An exemplary prior attempt to get a grasp on how some security works was already made in D2.2 (Overview of Security technologies) created within the EU FP7-funded research project PRISE (Privacy & Security), http://www.prise.oeaw.ac.at/publications.htm

public squares and buildings, streets, parks and other publicly accessible areas of the country. On the other hand, the surveillance of citizens in public spaces can be seen as an invasion of their privacy, and, where it is used to curtail citizens' rights, even as a foreboding of an Orwellian society.[7] The monitoring of public spaces is done mostly by visual or acoustic means. Owing to this fact, in this chapter we will describe technologies dedicated to public space surveillance with a focus on the two most relevant technological approaches: CCTV and drones.

2.1.1 Smart CCTV

In the wake of the terrorist events in September 2001, a multitude of surveillance technologies have been increasingly used for security purposes.[8] Closed Circuit Television (CCTV) has been one of them. And indeed, the deployment of CCTV technologies in numerous countries, including European Union member states, has been increasing ever since and continues to grow. However, while at first the terrorist attacks of 2001 triggered a worldwide political and societal desideratum to counter similar future dangers with the help of video surveillance, CCTV is becoming more and more common as a tool not only for simpler local crime prevention, but also for investigating minor offences.[9] Ideally, the national law of the respective countries foresees certain preconditions for the usage of public space visual observation, such as the fulfilment of a specific legal ground, the requirement of necessity, a legitimate purpose and the proportionality between the privacy impacts on citizens vs. the effectiveness of the measure to achieve the intended purpose.[10]

In this context, the current and on-going technological development of supportive and complementary elements like improved camera functions, facial as well as behavioural pattern recognition and other additional data matching capabilities make CCTV much more powerful than it has ever been. This "smarter" deployment of CCTV enables a significantly more comprehensive surveillance of citizens in public space areas, thus triggering a number of fundamental rights and privacy issues. Since law enforcement agencies increasingly use digital recordings as a security measure on a broader scale, there is also an increased risk of a surveillance atmosphere that permeates public space omnipresent and intrusive enough to affect citizens' lives in a manner which is disproportionate to the desired security enhancement. This effect is reinforced by the rise of advanced CCTV technologies in combination with an expansion of public spaces that are surveilled. Also, the costs of such increased public space surveillance are a point of criticism. So for example, in May 2012 the privacy campaign group Big Brother Watch sharply criticised the rise of police staff costs designated to oversee CCTV installations in London, which totalled £4.1m in 2011.[11] Also, another Freedom of Information request revealed that UK local authorities spent a total of £515m for the installation, operation and maintenance of public space CCTV surveillance in the years 2007 until 2011.[12] But irrespective of the costs, the implications of CCTV deployment such as privacy impact, effectiveness and social consequences provide ample opportunities for research and discussion. Thus, several research projects were initiated in the EU with focus on CCTV matters, e. g. the political, societal and security-related impacts of public space CCTV. Examples of such research projects are:

---

7 Cf. Nick Taylor in Surveillance & Society, V 1, N 1 (2002) "State Surveillance and the Right to Privacy", http://www.surveillance-and-society.org/articles1/statesurv.pdf

8 While this trend was definitely fuelled by the events of 2001, it already showed in the years previous to the attacks, cf. the article published June 21st 1997 by Privacy International, "CCTV Frequently Asked Questions", https://www.privacyinternational.org/blog/cctv-frequently-asked-questions

9 For an overview of the increasing deployment of CCTV from the global perspective until 2004, see Clive Norris, Mike McCahill and David Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", published in Surveillance & Society, vol. 2, no. 2/3 (2004), titled "The Politics of CCTV in Europe and Beyond"

10 Cf. the video surveillance guidelines by the European Data Protection Supervisor, published March 17th 2010, pp. 16 ff.

11 Cf. Nick Pickles, Big Brother Watch article published May 14th 2012, "London MET police spends £4m a year watching CCTV", http://www.bigbrotherwatch.org.uk/home/2012/05/met-cctv-4m-spendin.html

12 Cf. the Guardian Professional Networks article by Sade Laja published February 21st 2012, "Councils spend £515m in four years on CCTV", www.guardian.co.uk/government-computing-network/2012/feb/21/cctv-councils-big-brother-watch?INTCMP=SRCH

- ADDPRIV – Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance (http://www.addpriv.eu/)
- VANAHEIM – Video/Audio Networked surveillance system enhAncement through Human-cEntered adaptIve Monitoring (http://www.vanaheim-project.eu/)
- ADVISE – Advanced Video Surveillance archives search Engine for security applications (http://www.advise-project.eu/)
- Urbaneye Project (http://www.urbaneye.net/)
- 'Citizens, Cities and Video-Surveillance', a project initiated by the European Forum for Urban Security (http://www.cctvcharter.eu/)

Considering the findings of such research projects as well as further educational literature from various sources, this document will in the following describe the current state of the art and on-going research regarding CCTV technology. This will also include the combination with advanced equipment. In this context, the inherent privacy impact owing to the technical possibilities will be highlighted. Moreover, some thoughts on potentially Privacy-Enhancing Technologies (PETs) in the field of CCTV will be presented.

Standard camera construction types and functionalities

In this chapter, we will depict a broad range of such capabilities that are considered as a standard functionality for the foreseen application area. Taking a closer look at the governmental use of CCTV in this document, some classic deployment areas can be identified already. These are primarily the surveillance of buildings or facilities, public amenities (e. g. airports, train stations), the general hazard prevention in public places (especially at mass events[13]), traffic hot spots and the targeted monitoring of individuals for the purpose of hazard prevention or crime investigation. Depending on the intended application area of the CCTV camera (e. g. inbuilt in ATMs (automated teller machines), outside, inside etc.), the specific requirements regarding its technical capabilities may differ greatly.

The main function of CCTV cameras consists of recording visual signals, sometimes also audio signals, for a short or longer period of time. The cameras may show their input continuously, only within a specific time frame or at a specific event. The images can be watched during recording or afterwards, as long as the data are available. Possible storage media are video tapes, PC hard disks or digital video recorders (DVR) to provide for later (mostly forensic) use of the videos. Usually, these recordings are held accessible for a predefined time frame, after which they get archived, deleted or simply overwritten by newer recordings.

CCTV cameras may have various properties:

- Analogue or digital:
  Analogue cameras transmit analogue signals to a display and storage devices, digital cameras transmit digital signals. However, analogues signals can also be converted to digital signals which mostly come with a significant loss of image/video quality.
- Network connection:
  IP cameras or network cameras are connected to a server having an IP address, to which the signal is directly transmitted.[14] These network cameras do not need extra work steps to output

[13] For example, the London Olympics caused a massive rise of CCTV deployment in the area. According to the privacy campaign group Big Brother Watch, their Freedom of Information request resulted in the confirmation that 1,851 public-facing CCTV cameras on the Olympic Park and in the Olympic Village were installed at a cost of approximately £1,000 per camera. Cf. the group's website article written by Nick Pickles and published July 25th 2012, "Eyes on the Olympics", www.bigbrotherwatch.org.uk/home/2012/07/eyes-on-the-olympics.html

[14] Cletus O. Ohaneme, James Eke, Augustine C.O. Azubogu, Emmanuel N. Ifeagwu and Louisa C. Ohaneme, "Design and Implementation of an IP-Based Security Surveillance System", IJCSI International Journal of

their signal to an external medium since they are embedded into a server-based record system. The cameras are part of a LAN (wired network camera) or a WLAN (wireless network camera). The data transmission as well as a possible remote access to the recordings can usually be secured by encryption and authentication methods. Often IP cameras offer an enhanced image resolution.

- Image resolution:
  Standardised resolutions are defined for video formats, e. g. PAL (768 × 576 pixels) and NTSC (720 × 480 pixels), as well as computer graphics formats, e. g. VGA (640 × 480 pixels), SVGA (800 × 600 pixels) or SXGA (1280 × 1024 pixels). Megapixel cameras provide a resolution of at least a megapixel, e. g. SXGA. Meanwhile gigapixel cameras are available on the market.

- Mounting:
  There are various way of mounting the camera, e. g. dome cameras are situated in a dome, often at the ceiling, bullet cameras are inside a bullet-shaped housing, others are placed in boxes, discreet cameras are usually small and hidden at places where they are not visible as such, e. g. in equipment such as a clock, a smoke detector or in a doll. Cameras can be sheltered against vandalism.

- Pan-Tilt-Zoom:
  Cameras can come as a PTZ (pan-tilt-zoom) variant which enables a much more comprehensive camera vision of the surrounding area, the zooming functionality and the elimination of dead angles through the deployment of several devices with overlapping vision fields.[15] The zoom capabilities of such cameras already allow broad panoramic views while enabling zoom-in functions from up to several hundred meters.[16]

- Night vision:
  In low-light conditions, different technologies can support a night vision functionality of cameras, e. g., based on magnifying the existing light with Digital Slow Shuttering (DSS night vision cameras), by creating an own illumination source with a laser beam (laser illuminated cameras) or by infrared light (IR cameras) that provides thermographic recording of the surrounding and therefore does not show the real colours of the images.

- Thermographic:
  The thermal or thermographic camera works with infrared light to enhance the camera input by detecting black-body radiation coming from all objects, whereby a higher radiation level means higher object temperature. As part of the electromagnetic spectrum, infrared shows an image of the object (or subject) in different-coloured scales defined by warmth differences of the body areas independently from any external light conditions at the camera location, thus being able to operate even in total darkness, and to show sources of warmth or heat even if they are

---

Computer Science Issues, V. 9, I 5, N 1, September 2012, p. 393, accessible at: http://www.ijcsi.org/papers/IJCSI-9-5-1-391-400.pdf

[15] See the description in the research study conducted by Martin Gill & Angela Spriggs, employees of the Home Office Research, Development and Statistics Directorate, published February 2005, "Assessing the impact of CCTV", p. 12, accessible at: http://webarchive.nationalarchives.gov.uk/20110218135832/http://rds.homeoffice.gov.uk/rds/pdfs05/hors292.pdf

[16] To give an exemplary impression of today's possibilities, the panoramic image of the Vancouver Stanley Cup Final in June 2011, provided by the Vancouver Gigapixel Project, allows the tagging of individuals' faces over a distance of the far away back end of the Vancouver Canucks Fan crowd. Information on the high-res image and its tagging functionalities are available online at: http://www.gigapixel.com/image/gigapan-canucks-g7.html. Also see the article "Technology Is Our Friend ... Except When It Isn't" by James Fallows, published at theAtlantic.com August 27th 2011, and pointing out the dangers of such facial recognition in crowd sceneries to the exercise of civil liberties in public, available at: http://www.theatlantic.com/technology/archive/2011/08/technology-is-our-friend-except-when-it-isnt/244233/

behind walls. The disadvantage of such cameras is that their effectiveness is dependent on the surrounding temperature conditions to distinguish objects and subjects sufficiently.[17]

So, the current technical possibilities of CCTV standard equipment already enables the fine-grained identification of individuals at mass events, such as demonstrations, sport events etc. We will elaborate about the privacy and civil liberties implications of such possibilities later on in this chapter (Effectiveness of CCTV and civil rights impact). In the following chapter we will focus on the advanced equipment suited for the two former types to provide for a comprehensive overview.

Advanced CCTV equipment

CCTV solutions for public space surveillance come in various forms. First, a complete solution may be provided, meaning a complex system that includes all the hardware and software components which are required to accomplish a task. Also possible is the instalment of an add-on solution to already present CCTV surveillance systems, supporting multiple brands of cameras and enhancing the existing hardware and software capabilities. Such an add-on could enable hardware upgrades as well as the deployment of additional software docking onto the pre-existing software concept and supporting it. Another solution could be the compilation of a system tailored to a specific need and using only the necessary components, including hardware and/or software.

Within the research project ADDPRIV (Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance), an analysis and cataloguing of existing smart video surveillance solutions potentially relevant for integration with the algorithms developed in the ADDPRIV project was conducted. To achieve a comprehensive basis for the analysis, a number of commercial CCTV solutions from different vendors were examined and the advertised functionalities of these extracted. The results were then published in July 2011 in the deliverable D2.1 by the ADDPRIV consortium via the project website.[18] This specific document was analysed to obtain an overview of the current technical capabilities of modern CCTV camera systems. This analysis showed that nowadays CCTV systems can have a broad range of capture, record, storage and analytics capabilities that enable a much more extensive surveillance of public space areas.

In the following, the most important possible camera enhancement tools are listed for a quick overview[19]:

- Image stitching/fusion to create enlarged scenery images
- Real-time 3D display
- Video stabilisation
- High-resolution snapshots
- Instalment of recording schedules

---

[17] Cf. the definitions provided in the white paper of the commercial camera system vendor Vumii Inc., published September 2008, p. 3, "Continuous Wave Laser Illumination: The Clear Choice over Thermal Imaging for Long-Range, High-Magnification Night Vision Perimeter Protection", available as PDF at: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&ved=0CHUQFjAJ&url=http%3A%2F%2Fwww.securityinfowatch.com%2Fdownload%3Fcontent_id%3D10537280&ei=3pOKUPrQKMSK4gT68YDgBA&usg=AFQjCNFLB-RZbXBSrbksFfrsokYVXO-lOg&cad=rja and in the Wikipedia articles for thermal imaging camera (https://en.wikipedia.org/wiki/Thermal_imaging_camera) and Infrared (https://en.wikipedia.org/wiki/Infrared)

[18] For more details, see the document itself, titled "Deliverable 2.1: Review of existing smart video surveillance systems capable of being integrated with ADDPRIV project", submission date: July 31st 2011. It is publicly available as PDF under: http://www.addpriv.eu/uploads/public%20_deliverables/149--ADDPRIV_20113107_WP2_GDANSK_Scoreboard_R11.pdf

[19] Ibidem, see pp. 9 ff.

- Remote access of cameras from a central command station, laptop or any other specific mobile assistance device or through specific software
- GPS for position determination of said mobile assistance devices
- Joint work ability of different mobile assistance devices
- Camera status and functionality monitoring (covering camera failure and external sabotage events like camera hooding/masking/blinding, defocusing and repositioning)
- Integration of additional hardware and software components, e. g.
    - multiple sensor information,
    - analytics software,
    - wireless communication technology,
    - algorithms software support, e. g. for traffic control,
    - self-adaptive software to learn and react to the difference between typical and untypical subject- or object-related settings and situations (e. g. unusual behaviour of individuals, or different light and weather conditions)
- Distribution of the processing architecture to enhance system security and simplify installation and maintenance
- Synchronised retrieval and playback of multiple videos for forensics purposes
- Customisable alarm functions
- Combining triggers from multiple camera events in one alert
- Backup functionalities
- Sound and vibration detection
- Face detection
- Motion detection, including speed indicator
- Subject counting, even under high-density conditions
- Crowd detection
- Directional flow detection
- Unattended object detection
- Missing object detection
- Intrusion detection (also in 4D)
- Licence plate/number plate recognition
- Targeting of subjects or objects for position determination and route tracking
- 3D facial recognition
- Additional image processing software, e. g. for image quality enhancement such as shadow minimisation and reflection troubleshooting
- Audio support
- Data base storage connection and assistance, e. g. by real-time cataloguing content using XML and SQL

- Behavioural pattern recognition, classification, analysis and related alerts[20]

Beyond these possibilities, on-going research is seeking to develop new approaches to identifying and tracking individuals as well as classifying and analysing their behaviour. So for example, infrared CCTV cameras may under optimal conditions provide not only scenery vision, but also for an identification of individuals within the camera vision range. This is possible through facial recognition algorithms fed with biometric information defined by the thermal pattern of the individual's face appearing in the camera's vision range.[21] Another field of research is the deployment of improved algorithms to classify and analyse human behaviour. So for example, San Francisco's Municipal Transit Authority uses a self-learning algorithm developed and provided by the security firm BRS Labs to spot and react to anomalous behaviour. Deployed in the mass transit area, this algorithm includes behaviour patterns related to the time span of learned 'normal' behaviour in the surrounding area of the camera and extractions from it, such as loitering, tailgating, abandoned packages and abnormally high or low numbers of passengers. In this context, the velocity, acceleration and path of mass transit passengers passing through a station are also analysed. Moreover, the algorithm is able to learn the typical appearance of the camera surroundings and extractions from it, such as changes regarding colours, shapes, movement patterns, shininess and structures.[22]

Current research deriving from the military field concentrates on the classification of people's actions recorded by video cameras. This 'automatic action recognition' functionality matches certain actions of individuals to predefined action classes, such as the 'picking up', 'burying', 'digging out', and 'dragging along' of objects.[23] It is conceivable that this kind of recognition system may also get deployed outside the military context to enhance public security. Another example of emergent machine-driven behaviour classification possibly to be used in the Smart CCTV field results from the lively research using algorithms to recognise and classify human emotion. Such human emotion recognition systems can for example analyse facial expression and eye gaze as well as head and body movements of a person.[24] How far developed such algorithms are already, shows the newest achievements by the Affective Computing Group of MIT's Media Lab, which recently developed a facial recognition system which is able to distinguish between real and faked smiles.[25]

All of these aforementioned new research approaches represent a whole new dimension of CCTV surveillance aiming at being able to not only record the surroundings of the camera, but also to define what is going on in its vision area – or in its scope of audio capture. With working speech assistant

---

[20] Since this document is meant to give only an overview of the current and upcoming technical possibilities in the field of CCTV, a more detailed description and effectiveness analysis of the individual functionalities is unfortunately out of scope. However, the most interesting algorithms, namely object detection, object tracking, object classification, event detection, and route reconstruction were already described in detail within the ADDPRIV Deliverable 2.1 (pp. 45 ff.). Most of these algorithms are still subject to further research in this field, thus it is to be expected that even more advanced and effective techniques will be available in near future.

[21] Francine Prokoski, "History, Current Status, and Future of Infrared Identification", published in 2000 in IEEE Computer Society, Computer Vision beyond the Visible Spectrum: Methods and Applications, pp. 5-14, marathon.cse.usf.edu/~sarkar/biometrics/papers/IRSummary.pdf

[22] Fast Company web blog article by Neal Ungerleider, June 1st 2012, "Mass Transit Cameras Spot Bad Guys, No Human Judgment Required", http://www.fastcompany.com/1839052/big-brother-is-coding-you; see also the product description of BRS Labs on their website: http://www.brslabs.com/product-details.

[23] See Adi Robertson, theverge.com on October 28th 2012, "Military-backed surveillance prototype can read people's actions on video", www.theverge.com/2012/10/28/3567048/carnegie-mellon-video-surveillance-action-recognition

[24] An exemplary description of possible techniques was made by Yisu Zhao's thesis submitted to the Faculty of Graduate and Postdoctoral Studies, Ottawa-Carleton Institute for Computer Science, "Human Emotion Recognition from Body Language of the Head using Soft Computing Techniques", available at: ruor.uottawa.ca/en/bitstream/handle/10393/23468/Zhao_Yisu_2012_thesis.pdf?sequence=1

[25] MIT News web magazine, article by David L. Chandler, May 25th 2012, "Is that smile real or fake? A computerized system developed at MIT can tell the difference between smiles of joy and smiles of frustration.", http://web.mit.edu/newsoffice/2012/smile-detector-0525.html

systems for smart phones or devices such as Google Glass, the analysis of speech and its semantics has made great process, and biometric speech profiles of users are increasingly processed in clouds where a usage for other purposes may not be prevented.[26]

Further analysis might go beyond these steps to focus on event forecasting to predict certain actions of individuals. The ultimate goal in this context is the retrenchment of personnel who might no longer be needed to assess a certain situation displayed on a monitor. However, it is uncertain how long it will take until such algorithms are able to function faultlessly without triggering false alarms – if at all. Currently it seems that technologies for automatic identification of individuals and abnormal behaviour detection may produce acceptable results in very simple situations only, but are not performing in complex environment where they show poor accuracy. They fail due to the complexity of the scene. Eventually, the intelligence of trained security personnel will still be needed to ascertain the types of response required to different activated alarms.

Effectiveness of CCTV and civil rights impact

The effectiveness of Smart CCTV strongly depends on the reliability of its components and their functionalities – and it can only be reasonably measured when taking account the specific objective of the use case because there is no 'one size fits all' solution. This is particularly relevant for the algorithms developed for e. g. removed or left object detection or map/positioning since these functions depend on static cameras. This is because such algorithms rely on data gathering and computational processes to perform their function: The camera captures and 'learns' the typical appearance of its surroundings in its vision field. Within a predefined time frame, the camera (and its respective algorithm) performs image comparison techniques, thereby registering any changes that may have occurred to the scenery. But this technique automatically precludes a future deployment of mobile cameras owing to difficulties of adequate capture regarding the appearance of the surrounding area. Another weakness of such algorithms is the limited capability to process events in crowded scenery, owing to an increased signal input to be processed. However, this is a simple hardware obstacle that could be overcome with the accessibility of sufficient computing power and new big data techniques to perform the image processing.[27]

Nevertheless, the processing and analysis of image data may still prove faulty due to the difficulty of customising algorithms so they can deal appropriately with unforeseen events and behavioural pattern ambiguities.[28] Moreover, a significant weakness of current behavioural recognition algorithms is the fact that they are not yet able to independently detect and classify anomalous behaviour. Rather, these algorithms work to fashion a stereotypical predefinition of unwanted behaviour. So the predefined behaviour can be matched to any actions captured by the camera.[29] But typically, the deploying security agencies have no direct access to the underlying code of the algorithms deciding which behaviour is classified as 'abnormal'. So a potential deficit arises for ambiguous situations which are amplified through automated processing of behavioural patterns.

---

[26] David Talbot, "Wiping Away Your Siri 'Fingerprint'", MIT Technology Review, June 28th 2012, http://www.technologyreview.com/news/428053/wiping-away-your-siri-fingerprint/

[27] Currently, IBM is testing a new traffic-management technology in a pilot programme in Lyon, France, using big data to achieve a better performance of large data processing in traffic surveillance areas, Wired.com article by Doug Newcomb, published November 21st 2012, "How Big Data Will Ease Your Commute", www.wired.com/autopia/2012/11/big-data-commute/

[28] This leads to intensified efforts by vendors to provide improved software able to centralize different alarm sources and filter out relevant events needing human intervention; see for example the article in the Security Middle East Magazine issue 65 March/April 2012, titled "Improving situational awareness", http://www.securitymiddleeastmagazine.com/features/view/32

[29] This is for example a weakness of the aforementioned "automatic action recognition" functionality, which pre-determines certain actions of individuals and thus is not yet able to ascertain unforeseen activities of individuals, see the article by Adi Robertson, "Military-backed surveillance prototype can read people's actions on video"

Ultimately, however effective the above-described functionalities of Smart CCTV are, the largest potential for technical failure remains within the area of the overall configuration of the camera system. Whenever the accuracy of the camera data is in question, the specific set-up, management and usage of said device is a crucial factor, deciding the chances of the technology to achieve its deployment purpose.[30] For example, also poor positioning, lighting and weather conditions are a challenge for most cameras, depending on their specific capabilities, and will produce low-quality image results. Additionally, angle/perspective issues may influence the results of facial-recognition techniques strongly, as well as hindrances in capturing the individuals' faces due to the usage of hats or sunglasses.[31]

Regarding the impact of public space surveillance by the means of Smart CCTV, the most important issues are the implications with regard to human rights matters. According to Benjamin J. Goold, CCTV by its very nature undermines citizens' fundamental right to privacy in public deriving from several legal sources, one of the clearest being Article 8 of the European Convention on Human Rights. The duration, intensity and potential consequences of CCTV data collection, processing and storage by the state instil a feeling of uncertainty in the individuals being observed. This uncertainty can lead to more or less subtle changes in behaviour to avoid attention. This effect is even more inherent with the rise of behavioural/anomaly pattern recognition functionalities in newer CCTV systems. These are not yet able to classify the behaviour of individuals faultlessly, thus increasing the risk of becoming the focus of attention with just unusual but still legal behaviour.

So such Smart CCTV systems definitely have the potential to suppress any kind of out-of-the-norm behaviour of citizens. This consequently might discourage citizens from exercising their own fundamental rights, such as privacy, freedom of expression and freedom of association, with an even stronger impact on citizens belonging to any kind of minority or suffering from the stigma of being an outsider.[32] This feeling of being visible and observed might not only be unpleasant for persons having experienced mobbing, stalking or discrimination in their lives. Looking at the often most-intended purpose of CCTV deployment, which is the prevention of crimes in public space areas, several studies have shown that the visual surveillance does not have the desired effect with regard to certain types of crime. For instance, affective deeds are born out of the heat of the moment and often are influenced by the consumption of alcohol. Thus, the observation of individuals with cameras is not suited to preventing sudden violence during interpersonal encounters.[33]

Moreover, the broad surveillance of public space might invade the privacy of individuals in a fashion that even especially sensitive personal information is concerned. This is most often the case if doors and windows of certain offices and institutions where any kind of professional secrecy plays a role are also within the visual range of the CCTV camera. Also, capabilities of the CCTV systems with regard to audio

---

30 Such failures caused by the false analysis of camera data is described on the basis of a case study by Alex Stedmon in his article "The camera never lies, or does it? The dangers of taking CCTV surveillance at face value and the importance of human factors", Surveillance & Society, vol. 9, no 3 (2012), "Urban Surveillance", http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/4192/4194; see also the article by SA Mathieson and Rob Evans for The Guardian, "Roadside cameras suffer from large gaps in coverage, police admit", August 27th 2012, http://www.guardian.co.uk/uk/2012/aug/27/police-number-plate-cameras-network-patchy

31 These weaknesses were also described in the ADDPRIV "Deliverable 2.1: Review of existing smart video surveillance systems capable of being integrated with ADDPRIV project", see p. 45.

32 See the further elaborations on this topic made by Benjamin J. Goold, University of British Columbia, in "CCTV and Human Rights", pp. 27 ff.; this article was published in the "Citizens, Cities and Video-Surveillance", paper of the European Forum for Urban Security publication of June 2010, titled "Citizens, Cities and Video Surveillance – Towards a democratic and responsible use of CCTV", www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_publication_EN.pdf

33 Peter Squires, Professor of Criminology and Public Policy at the University of Brighton examined the results of such studies in his article "Evaluating CCTV: Lessons from a Surveillance Culture", published on pp. 39 ff. in the "Citizens, Cities and Video-Surveillance", paper of the European Forum for Urban Security publication of June 2010, titled "Citizens, Cities and Video Surveillance – Towards a democratic and responsible use of CCTV"

recordings must be considered in this context. So, for a CCTV surveillance to be non-invasive, it must be ensured that the secrecy obligations, e. g. of doctors, lawyers, psychologists, and trade unions, are not endangered.

Another critical factor of CCTV surveillance is the security of the CCTV system as a whole or in its critical parts. Critical vulnerabilities in newer CCTV systems are e. g. the network transmission security, the security of the servers where the data are processed and stored, or the security of the remote web-based access. So, appropriate safeguards are needed to prevent data leaks or breaches. As for a tangible example regarding technical security issues, the German Data Protection Commissioner for the Federal State of Niedersachsen demands a specific examination regarding the necessary preconditions to enable a secure deployment of wireless security cameras. The wireless transmission of the image data occurs typically in a freely accessible 2.4-GHz range, which is also used e. g. by Bluetooth and WLAN devices for communication. Consequently, each receiving station within transmission range is potentially able to receive the respective signals, enabling either open or covert recording of the data. But the legality of the collection, transmission and reception of such video image data might always be questionable. So it is advisable to implement appropriate technical and organisational measures and to consider effective approaches to Privacy by Design before and during the set-up of a CCTV solution.[34]

Potential Privacy by Design approaches

Aligned with the core idea of Privacy by Design and the related concepts of Cavoukian and the Danish National IT and Telecom Agency Copenhagen presented in Chapter 1 of this document (Methodology and Concepts), some realisation measures in the field of CCTV as well as Smart CCTV are conceivable. These could, for example, be encryption techniques, comprehensive authorisation/access concepts and correlating access controls, including secure credentials and also logging functions for auditing/forensics. More tangible examples may be derived from the practical execution in individual use cases and specifically tailored privacy-enhancing CCTV solutions offered by several vendors. A precise examination of the camera's pan, tilt and zoom capabilities may be made with the issue of citizens' privacy in mind. Also, a specific set-up regarding camera location, viewing angles, number of cameras, and time of monitoring, image quality and resolution may be a good first step to minimise the data collection to the level absolutely necessary.[35] Similarly, collection of audio data should be minimised.

In this context, the exclusion of certain areas not relevant for the intended surveillance purpose might also be executed by pixelating, blurring, blackening, obfuscating or masking of the non-relevant areas within camera vision. This concerns persons and objects as well as sensitive areas within camera vision range. Such a process makes it possible to prevent the identification of individuals within camera vision range or to hinder the recording of areas belonging to private property.[36] However, dependent on which concept is realised, the process may still be reversible. So more preferable would be a method that does not record the areas in the video in the first place. If this is not possible, the access to the excluded parts must at least be tightly restricted to provide for consistent data protection compliance.[37]

---

[34] The Data Protection Commissioner of Niedersachsen, Germany, website publication "Funk-Überwachungskameras – ein häufig unterschätztes Problem" (translated: "Wireless surveillance cameras – an often underestimated problem"), available in German at: http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=13098&article_id=56224&_psmand=48

[35] Cf. the EDPS Video Surveillance Guidelines by the European Data Protection Supervisor, published March 17th 2010, pp. 24 ff.

[36] Cf. the Decision of the German Federal Administrative Court of January 25th 2012, (Az. BVerwG 6 C 9.11). The court decided that the capture of private property during a public space surveillance at the Hamburg Reeperbahn in Germany, where window, door and balcony images of a citizen's house was made, is unlawful and violated the concerned citizen's right to informational self-determination and privacy. The court determined that these sensitive areas of private property should be excluded from the surveillance measure.

[37] Several vendors have already specialized on such privacy-enhancing features. The KiwiVision Privacy Protector system, developed by the KiwiSecurity Software GmbH, provides an algorithm for anonymising video data by obfuscating persons, objects or fixed regions within camera vision range. Still, the obfuscating process is

So to provide a summary of the above-described measures and to mention further exemplary methods supporting the privacy-friendliness of CCTV solutions, some possibilities of inbuilt Privacy by Design are:

- Exclusion of sensitive areas, e. g. windows with a view into private property, by obfuscating, masking etc. or limiting the zooming-in functionality
- Limitation of camera record to only relevant events (e. g. left luggage)
- Excluding or limiting audio surveillance
- De-identification of individuals (pixelating, blurring, blackening, obfuscating, masking)
- Limiting the time frame of surveillance measure deployment
- Secure communication between cameras and display/storage/analysis units
- Encrypted storage media
- Access controls regarding video records and reversibly excluded parts
- Access logging
- Appropriate data breach notification process
- Automated deletion routines aligned with specified time periods (legal deletion deadline at the latest)
- Improved accuracy, e. g. of analytics algorithms to prevent/minimise false positives and false negative alarms
- Documentation of privacy and security analysis of the full (Smart) CCTV System and deployed measures for evaluation[38]
- Transparency on whether and in which scope the camera is recording data, and information on the responsible data controller
- Regular privacy and security audits of all components including the analytics algorithms

This list is by no means conclusive. Rather, an analysis of and decision about the measures needed must be conducted per individual case on the basis of the intended purpose, the necessity of the technology and the area where the camera will be located. So, a use case based Privacy Impact Assessment (PIA) might be beneficial to eliminate or at least reduce the infringement on citizens' fundamental rights at an early stage of the measure implementation. Moreover, it is advisable to consult a data protection authority during a process of prior checking before implementing new CCTV systems.

2.1.2 Drones

Drones are, like Smart CCTV, a technical approach to conducting the surveillance of public spaces for the purpose of enhancing security. They represent the latest domestic application of a technology first employed in the military field during World War I; the first earnest deployment of an unmanned aerial vehicle was Archibald Montgomery Low's 'Aerial Target' in 1916.[39] However, drones gained greater public attention when an armed drone became known to have been involved in the targeted killing of

reversible, whereas the access is restricted (for more details, see https://www.european-privacy-seal.eu/awarded-seals/de-090017). The Multieye PrivacyShield, developed by the software company artec technologies AG, works similarly. For details see http://www.artec.de/de/produkte/multieye/module-lizenzen-zubehoer/multieye-privacyshield.html.

38 The EDPS Video Surveillance Guidelines, European Data Protection Supervisor, March 17th 2010, pp. 37 ff.

39 Gary C. Warne, "The Predator's Ancestors – UAVs in The Great War", July 25th 2012, http://warnepieces.blogspot.de/2012/07/the-predators-ancestors-uavs-in-great.html

high-ranking Al-Qaeda military commander Mohammed Atef in Afghanistan in November 2001.[40] Since then, the U.S. have used unarmed as well as armed drones in a number of foreign countries beyond Afghanistan (e. g. in Pakistan, Yemen, Somalia and Iraq) and also in the domestic area in different contexts and for different reasons. More than 70 other countries worldwide have followed this example and now use this new technology for a variety of purposes.[41]

Drones are generally referred to as Unmanned Aerial Vehicles (UAV) or Unmanned Aerial Systems (UAS). In fact, more than 1,000 UAV systems exist today worldwide.[42] In Europe, engineers at EADS Cassidian are developing a drone with a 40-meter wingspan, based on the Global Hawk model of Northrop Grumman; the Euro Hawk, as it is to be named, completed its first successful test flight in January 2013.[43] In the United States, larger drone types from the military field are referred to as Remotely Piloted Aircraft Systems (RPAS) to highlight the fact that these drone systems are always controlled by a human operator. Drones are remotely controlled, either by a pilot from a ground location or by pre-programming.[44] The remote controlling typically does not only include the flight operation, but also the additional technical capabilities the machine might be equipped with.[45]

Though initially being designed for purposes of military reconnaissance and targeted strikes with weaponry, drones may also be deployed in a multitude of different areas. These areas may be quite widespread and range from commercial uses to governmental law enforcement deployment. So for example, Russian archaeologists used a miniature drone to create a 3D model of an ancient burial mound in a remote and rugged area in Tuekta, Russia.[46] Other potential uses can be found in the field of geographical land surveying. Beyond this, in the Antarctic seas, eco-activists have started using drones to track and monitor illegal whaling ships.[47] Moreover, the World Wildlife Fund (WWF) received funding from the U.S.-based company Google for the further investment in unmanned aerial vehicles to be used worldwide for protecting endangered animal species by tracking and deterring illegal hunters.[48]

Sometimes there are overlaps between purely scientific and security-related uses of drones. An example of such an overlap is the drone being used by safety inspectors in Japan's nuclear power plant

---

40 Cf. Micah Zenko, Douglas Dillon Fellow, "9/11 Lessons: Unconventional Warfare", article published August 26th 2011 for the Council on Foreign Relations website, http://www.cfr.org/united-states/911-lessons-unconventional-warfare/p25661

41 According to the unclassified version of the U.S. Government Accountability Office (GAO) report on the proliferation of UAVs of July 2012, the number of countries using drones has increased between 2004 and 2011 from 41 to 76, see p. 9

42 Melih Cemal Kushan, Faculty of Engineering and Architecture, Eskisehir Osmangazi University, Eskisehir, Turkey, "The relationship between the UAV fleet of European countries and their geopoliticial position" publication for the International Conference of Scientific Paper AFASES 2012, Brasov, 24-26 May 2012, http://connection.ebscohost.com/c/articles/82405348/relationship-between-uav-fleet-european-countries-their-geopolitical-position

43 Andre Tauber for Die Welt, "Die Superdrohne ist ein riesiger Datenstaubsauger" (translated: "The super drone is a giant data hoover"), available in German at: http://www.welt.de/wirtschaft/article112713975/Die-Superdrohne-ist-ein-riesiger-Datenstaubsauger.html

44 Though drones are mostly known for being used in aviation, there are also unmanned vehicles known to operate on the ground and under the sea.

45 Cf. the definition of the U.S. Department of Defence, which sees a drone, also called unmanned aircraft, as "an aircraft or balloon that does not carry a human operator and is capable of flight under remote control or autonomous programming", 331 Joint publications 1-02, Dictionary of military and associated terms (2010), amended July 15th 2012.

46 Charles Choi for LiveScience, "Tiny Drone Reveals Ancient Royal Burial Sites", October 7th 2011, http://www.livescience.com/16443-micro-drone-archaeology-burial-sites.html

47 Jonathan Franklin for The Observer, "Whaling: campaigners use drones in the fight against Japanese whalers", January 1st 2012, http://www.guardian.co.uk/environment/2012/jan/01/drones-fight-japanese-whalers

48 Dana Liebelson, "Google-Funded Drones To Hunt Rhino Poachers", December 5th 2012, http://www.motherjones.com/blue-marble/2012/12/rhino-poacher-meet-drone-funded-google

Fukushima Daiichi in order to conduct a remotely controlled survey of the tsunami damage.[49] In 2011, first test runs were conducted with a 3-ft-long, 8-lb GALE drone designed to fly into hurricanes to record and transmit data useful for hurricane forecasts.[50] In Germany, Israeli Heron drones are under consideration for use in maritime search and rescue, for detecting environment polluters and for the surveillance of influxes of refugees via sea routes.[51] In the U.S., several governmental agencies have requested a licence for drone deployment to observe forest fires and avalanches. In Europe, research is also aiming at optimising the usage of drones for search & rescue as well as disaster relief missions. So for example, in the context of the EU-funded project NIFTi (Natural human-robot cooperation in dynamic environments), the Fraunhofer Institute, Department for Intelligent Analytics and Information Systems (IAIS), provides an octocopter drone for the integration for research work on human–robot cooperation in dynamic environments.[52]

More conventional security-focused uses of drones derive from typical law-enforcement purposes, such as searching farm fields in rural areas for illegal crops, drug production and trafficking, as well as aerial observation of houses during high-risk police operations.[53] In Croatia, the start-up company Hypersphere offers UAVs in the form of 20-meter-wide, helium-filled airships designed for border control purposes.[54] European research continues in the field of border control, with the EU agency Frontex being tasked with the promotion, coordination and development of an integrated European border management in line with the EU fundamental rights charter. This also involves assessing the viability of Remotely Piloted Aircraft Systems in providing enhanced surveillance coverage of long stretches of land and sea borders. Frontex is also part of the European Border Surveillance System (EUROSUR).[55] Moreover, the EU-funded project OPARUS (Open Architecture for UAV-Based Surveillance System) aims towards an open architecture for the operation of unmanned air-to-ground wide-area land and sea border surveillance platforms in Europe.[56]

Already in 2008, heated public discussion focused on the intentions of governmental security agencies to not only use surveillance drones against hooligans during soccer events, or for securing Castor transports, but also for observation and CCTV recording at political demonstrations.[57] Such uses for drones are considered valid for many security agencies worldwide, whereas their legality is yet subject of intense expert discussions. In the United Kingdom, drones were used as a preventive counter-terrorism measure at the 2012 Olympics in London by observing the sky during the games.[58] Looking at

---

[49] Matt Smith for CNN, "Flying drone peers into Japan's damaged reactors", April 10th 2011, http://articles.cnn.com/2011-04-10/world/japan.nuclear.reactors_1_radioactive-water-tokyo-electric-power-reactors?_s=PM:WORLD

[50] Ken Kaye for the Los Angeles Times, "Tiny aircraft could improve hurricane forecasts", September 30th 2011, http://articles.latimes.com/2011/sep/30/nation/la-na-hurricane-drone-20111001

[51] Ulrich Clauß for Die Welt, "Bundespolizei erprobt Drohnen beim Küstenschutz" (translated: "Federal police testing drones for coastal protection"), December 28th 2012, available only in German at: http://www.welt.de/politik/deutschland/article112252357/Bundespolizei-erprobt-Drohnen-beim-Kuestenschutz.html

[52] For more details on the approach and use cases, see the project website at: http://www.nifti.eu/ and a field report presentation on Rescue Robots used in the earthquake-hit region of Mirandola, Italy, available as PDF under: http://www.nifti.eu/results/2012.mirandola.pdf

[53] Cf. Jennifer Lynch for Electronic Frontier Foundation, "Newly Released Drone Records Reveal Extensive Military Flights in US", article of December 5th 2012 describing a range of domestic drone uses in the U.S., https://www.eff.org/deeplinks/2012/12/newly-released-drone-records-reveal-extensive-military-flights-us

[54] Ben Rooney, The Wall Street Journal, "Airship Plan to Put Cameras in the Sky", November 19th 2012, http://blogs.wsj.com/tech-europe/2012/11/19/croatian-airship-plan-to-put-cameras-in-the-sky/

[55] http://www.frontex.europa.eu/

[56] http://www.oparus.eu/

[57] Carsten Lißmann for Zeit Online, "Die unsichtbaren Ermittler" (translated: "The invisible investigators"), January 1st 2008, http://www.zeit.de/online/2008/03/unbemannte-drohnen-hooligans-sachsen; Lorenzo Franceschi-Bicchierai, Wired.com, "Russia Is Stockpiling Drones to Spy on Street Protests", July 25th 2012

[58] Greg McNeal for Forbes.com, "London Olympics Security Focuses on Deterrence: Use of Drones, Electric Fences, Missiles and More", June 23rd 2012, http://www.forbes.com/sites/gregorymcneal/2012/07/23/london-olympics-security-focuses-on-deterrence-use-of-drones-electric-fences-missiles-and-more/

much smaller-scale uses of drones for security, some private companies also envision an overlap between their commercial interests and potential security-enhancing capabilities of drones. In December 2012, a Japanese security firm revealed plans of renting out a company-designed drone for use in private homes to take off at intrusion-alarms for recording break-ins in real-time.[59]

Summarising all of these not conclusively mentioned potential uses for drones, it can be said that irrespective of the individual purposes, the deployment of UAVs has become a solid reality in Europe as well as worldwide. And the importance of drones will continue to increase as private companies, universities and other research entities as well as state and local agencies find more uses for drones in different fields. Looking at Europe, especially civil drones, as they fall under the EU's definition of Remotely Piloted Aircraft Systems (RPAS), are nowadays allowed in segregated airspace or in line of sight only. But it is to be expected that use of such civil drones will significantly increase in the near future, since the European Commission demanded the opening of civil airspace of the 27 member states for these RPAS, including drones, by 2016.[60]

In this document, we will, owing to the project scope, focus on a description of drones used for security purposes only. Thereby, we may take into account some developments in the military field, as far as they may also be influential for a potential domestic deployment.

Drone construction types and flying abilities

What is common for all types of drones is that, since they are unmanned, they are usually remotely controlled by ground personnel controlling the activities of the vehicle. In some cases, it may be possible to pre-program a drone for a specific flight route within its range. Compared to remote piloting, the autonomous programming of such drones is still in its infancy and the focus of current research, which we will also tackle in the following subsections. However, a remotely controlled drone needs a ground station, either fixed or mobile. This way, a tablet or a smartphone can nowadays easily be configured to function as a drone control device.[61] The communication between drone and operator may occur in various forms, though, for long-range distances, a satellite link may be needed to support the transmission of visual or other data from the vehicle and to relay commands back.[62]

Summarising the above, an UAV system consists of these elements:

- Unmanned aircraft (UAV)
- Ground control unit, possibly mobile
- Data link, possibly with satellite support
- Additional equipment

There are a number of drones in a great variety of sizes and designs. The size of a drone may vary greatly; one of the largest, most commonly known drone types would be the U.S. Reaper drone, with a wingspan of 20 meters, and a cargo capacity of 1,700 kg overall.[63] Currently deployed for mainly domestic uses, however, are the middle- to small-sized drones, often in the form of 4-rotor-equipped

---

59 AFP at Phys.org, "Japan security firm to offer private drone", December 27th 2012, http://phys.org/news/2012-12-japan-firm-private-drone.html

60 European Commission staff working document "Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)", SWD(2012) 259 final, September 4th 2012, available at: http://www.uasvision.com/wp-content/uploads/2012/09/EC_SWD_Euro-Strategy-RPAS_120904.pdf

61 In September 2011, Boeing engineers joined forces with MIT students to build an iPhone app that can control a drone from up to 3,000 miles away, cf. Jesse Emspak, "iPhone Flies Drone From 3,000 Miles Away", September 28th 2011, http://news.discovery.com/tech/apps/iphone-flies-drone-3000-miles-away-110928.htm

62 Cf. BBC News South Asia, "Drones: What are they and how do they work", January 31st 2012, http://www.bbc.co.uk/news/world-south-asia-10713898, and Salman Siddiqui, "Celebrating Paksat-1R: Pakistani drones – a dream or reality", August 6th 2012, http://tribune.com.pk/story/418118/celebrating-paksat-1r-pakistani-drones-a-dream-or-reality/

63 Cf. the U.S. Air Force fact sheet website for the MQ-9 Reaper drone, http://www.af.mil/information/factsheets/factsheet.asp?fsID=6405

quadcopters used for specific surveillance purposes.[64] Even smaller drones, called micro or nano drones, are currently being developed, though these are deployable in a limited number of use cases so far, owing to their small size and range.[65] The nano drones are often inspired by biology and imitate the movement of birds or insects.[66]

There are several approaches to classifying the various drone types, based on different criteria. One way to categorise these machines would be related to their field of use, and referring to their purpose. Other criteria focus on specific designs. According to these approaches, the most mentioned types of drones are:

- Large-sized military drones equipped with weaponry
- Smaller tactical military drones for reconnaissance
- Drones designed for logistics and carrying cargo
- Law-enforcement drones
- Civil and commercial drones
- High-altitude, long-endurance drones
- Bio-inspired drones
- Swarm-flight drones
- Supersonic drones & rocket-launched[67]

The most widely known categorisation of drones is the United States military tier system.[68] Similar categorisations are also used in Europe. However, according to classifications being made at events of the ParcAberporth Aerial Unmanned Systems forum, it appears logical to focus on range and altitude details of the unmanned vehicle. To mention only the first three categories out of nine of this classifications because the further categories are outside of the SurPRISE project's scope:

- Hand-held 2,000 ft (600 m) altitude, about 2 km range
- Close to 5,000 ft (1,500 m) altitude, up to 10 km range
- NATO type 10,000 ft (3,000 m) altitude, up to 50 km range
- ...

The flight duration of unmanned vehicles varies greatly, depending on their size and energy supply. There may be different ways to provide a drone with flight energy. Due to their greater altitude capabilities, the larger drones may rely on combustion engines to fuel their flight. In contrast, smaller types for near-range and limited-time uses are mostly powered by rechargeable batteries. However, the duration of the battery power is often very limited. Current research is aiming at techniques to refuel or recharge drones in the air during an operation.[69]

---

64 Liz Hull, Mail Online, "Drone makes first UK 'arrest' as police catch car thief hiding under bushes", February 12th 2010, http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html

65 See also Susanne Posel, elaborating in her article about current research focusing on insect-shaped micro drones, "The Insects Are Watching: The Future of Government Surveillance Technology", http://amresolution.com/2012/06/18/the-insects-are-watching-the-future-of-government-surveillance-technology/

66 Spencer Ackerman for Wired.com, "Air Force Keeps 'Micro-Aviary' Of Tiny, Bird-like 'Bots", February 11th 2011, www.wired.com/dangerroom/2011/11/air-force-micro-aviary-drones/

67 Alexandra Gibb, "A Drone Field Guide", May 31st 2012, opencanada.org/features/the-think-tank/graphic/a-drone-field-guide/

68 Cf. the Wikipedia entry at http://en.wikipedia.org/wiki/U.S._Military_UAV_tier_system for a rough overview of the variants of the U.S. military tier classification system.

69 So for example, the DARPA has conducted several close-proximity flight tests with two modified RQ-4 Global Hawk UAVs to explore the possibilities of autonomous aerial refuelling (press release of the Pentagon's Defense Advanced Research Projects Agency (DARPA) of October 5th 2012, "Making Connections At 45,000 Feet: Future UAVs May Fuel Up In Flight", http://www.darpa.mil/NewsEvents/Releases/2012/10/05.aspx). The U.S. defence supplier Lockheed Martin conducted tests with their Stalker UAS to demonstrate a laser-powering system to recharge the vehicle's energy supply and extend the flight duration up to 48 hours (press release on the website

Other interesting research developments aim at making the drones less dependent on human supervision, crossing the boundaries to robotics sciences. Sensors to estimate the proximity to geographical barriers and hindrances as well as pre-programmed navigation functions such as waypoint following might in the future enable smaller drones to independently find their way in urban cityscapes. This also counts for small micro drones being designed with swarm flight abilities. In 2012, robotics researchers at the University of Pennsylvania released a video of their nano quadrotors, each equipped with its own proximity sensors, doing synchronised formations and flying through a mock-up window to perform the collective dodging of hindrances.[70]

Currently, the main research areas related to the autonomy of drones can be divided into a number of different categories, which are:

- Sensor fusion
  - The combination of multiple sensor information from different sources
- Communications
  - Communication and coordination handling between multiple agents, taking into account incomplete and imperfect information
- Motion planning (also called path planning)
  - Path optimisation for the drone, taking into account certain objectives and constraints
- Trajectory generation
  - Control manoeuvre determination for a predefined path or to a specified location
- Task Allocation and Scheduling
  - Optimal task distribution taking into account time and equipment constraints
- Cooperative Tactics
  - Sequence formulation and spatial activity distribution optimisation between agents[71]

At least some smaller types of drones are already available for civil use at low cost and with little effort. In 2011, University of Southampton engineers built a drone, for which the single construction parts can easily be assembled by using a laser 3D printer.[72] New ways for the mass-production of micro drones are also in the making. For example, at the Harvard School of Engineering and Applied Sciences, a production method was developed which is inspired by children's pop-up books, enabling a swift fabrication of insect-like nano drones [73] Overall, it can be said that the technological capabilities in the

---

of Lockheed Martin of July 11th 2012, "Laser Powers Lockheed Martin's Stalker UAS For 48 Hours", http://www.lockheedmartin.com/us/news/press-releases/2012/july/120711ae_stalker-UAS.html). Other approaches focus on the implementation of hybrid turbine-electric propulsion systems (Graham Warwick on Ares Defense Technology Blog, "Hovering Near You – IARPA's Quiet UAV", July 18th 2012, http://bit.ly/OpUkWW (http://www.aviationweek.com/)). New research by a Mexican start-up aims at the distribution of a solar-powered six-foot-long drone able to conduct surveillance for up to 14 hours (David Ferris, "This Solar-Powered Drone Will Watch You All Day", Forbes article of August 16th 2012, http://www.forbes.com/sites/davidferris/2012/08/16/this-solar-powered-drone-will-watch-you-all-day/).

70 University of Pennsylvania, General Robotics, Automation, Sensing and Perception (GRASP) Laboratory, http://www.youtube.com/watch?feature=player_embedded&v=YQIMGV5vtd4

71 Kushan, "The relationship between the UAV fleet of European countries and their geopoliticial position", p. 2

72 Glenn Harris, "Southampton engineers fly the world's first 'printed' aircraft", July 28th 2011, http://www.eurekalert.org/pub_releases/2011-07/uos-sef072811.php

73 Cf. Harvard School of Engineering and Applied Sciences website article "In new mass-production technique, robotic insects spring to life", February 15th 2012, http://www.sciencedaily.com/releases/2012/02/120215155309.htm

field of unmanned aerial vehicles are developing quickly. Also, construction, deployment and costs become increasingly faster, cheaper and more efficient.

Advanced drones equipment

As explained above, Unmanned Aerial Systems do not comprise only the flying machine itself with its human pilot controlling remotely. Rather, the drone may also be equipped with additional features. What kind of add-on is possible depends on the size and payload capability of the individual vehicle. To give a short overview, these include:

- Smart CCTV equipment, including all possible features of CCTV, e. g. facial recognition, infrared/thermal imaging cameras, audio recording, and behavioural pattern recognition (cf. Chapter 12.1.1 'Smart CCTV')
- Panoptic equipment, enabling the surveillance of larger areas and the tracking of a high number of individuals or vehicles[74]
- Different types of radar technology[75]
- Wi-Fi interception technology[76]
- Other wireless communication surveillance technology and GPS (cf. Chapter 2.2.4 'Location Trackers')
- Hub for own communication[77]
- Chemical or radiation measurement[78]
- Armoury-like projectiles, explosives, electro-shockers, tear gas dispensers or firearms (lethal/non-lethal)[79]

Concluding, it can be stated that drones may be provided with a great variety of different add-on equipment, enabling surveillance as well as intervention. It is yet to be seen which further uses can be found for technology equipment in the context of unmanned aviation.

Effectiveness of drones and civil rights impact

For the time being, the main feature of drones which draws attention to them is the sound of their propulsion motors. Usually, most of the larger drones make a deep, loud buzzing sound, whereas rotors

---

[74] This refers to the so-called ARGUS-IS project or the Gorgon Stare project. For example, the Autonomous Real-Time Ground Ubiquitous Surveillance-Imaging System (ARGUS-IS) provides a "1.8 gigapixel camera system with 65 independent and steerable 'windows' that allow operators to survey 36 square miles at once", cf. Arnie Heller, Science & Technology Review, issue April/May 2011, "From Video to Knowledge" https://str.llnl.gov/AprMay11/vaidya.html; the Gorgon Stare project focuses also on a video capture technology, whereas a cluster of up to 12 cameras is attached to an aerial drone, performing wide-area sensor surveillance, cf. Ellen Nakashima and Craig Whitlock for The Washington Post, "With Air Force's Gorgon Drone 'we can see everything'" January 2nd 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html

[75] For examples of radar and sensor technology estimating proximities, cf. Kevin McCaney, "Army's 'sense and ' radar will let drones fly in domestic airspace" July 10th 2012, http://gcn.com/articles/2012/07/10/army-sense-avoid-radar-gbsaa-drone-technology.aspx

[76] Kim Zetter, "DIY Spy Drone Sniffs Wi-Fi, Intercepts Phone Calls", August 4th 2011, http://nonviolentconflict.wordpress.com/2012/03/09/diy-spy-drone-sniffs-wi-fi-intercepts-phone-calls/

[77] This is one of the functionalities intended for the DARPA underwater drone, see Alexis Santos, "DARPA unveils plans for undersea payloads that surface on command"

[78] Cf. Owen Bowcott and Nick Hopkins for The Guardian, "Future is assured for death-dealing, life-saving drones", August 4th 2012, http://www.guardian.co.uk/world/2012/aug/04/future-drones, and the AFP article in the Sydney Morning Herald of June 13th 2012, "Japan to develop drones to monitor radiation", http://www.smh.com.au/technology/sci-tech/japan-to-develop-drones-to-monitor-radiation-20120613-208zs.html

[79] Reuters article of March 14th 2012, "Police drones to be equipped with non-lethal weapons", http://rt.com/usa/news/drone-surveillance-montgomery-weapon-507/

of smaller quadcopters can be recognised by a high-pitched hum.[80] This attribute may diminish the operational capability of drones in cases where individuals are to be observed covertly. With larger drones, this problem may be unimportant since some of them have the ability to surveil effectively from a higher position in air, thus keeping enough distance so that they won't be noticed. Still, this places some restraints on drone uses for covert surveillance, so researchers are working on the development of noise-reduced UAVs.[81]

As already described above, drones have different construction designs and appliances to provide them with sufficient energy for flight. However, these also put limits on their capabilities regarding altitude, speed and duration of flight. But we also described above that efforts are taken to improve the energy supply capabilities and processes (e. g. by autonomous refuelling or re-charging during flight).

A much more significant problem exists with regard to the advanced CCTV equipment of drones. Details of visual CCTV footage often remain blurry owing to the movement of individuals surveilled and the drone itself, as well as inadequate capture angles. Images most often appear usable only if the drone directly hovers over the object or subject to be recognised.[82] Moreover, all the other restrictions and drawbacks of CCTV technologies, which we described in Chapter 2.1.1, also apply. Furthermore, the data collected by CCTV and sensors create a heavy workload, which is not yet resolved adequately by complementary automated data filtering or processing techniques. Also, bandwidth is an issue.

The targeting of an individual, or a group of individuals, occurs with the aid of CCTV/infrared cameras and sensors the drone is equipped with. However, the satellite data transmission between the capturing devices on the drones and the ground station displaying the images on screen for the ground-based pilot is mostly somewhat delayed. This delay, also called 'latency', makes it possible for targeted persons to avoid precise actions against them by moving around as much as possible.[83] The latency time is also responsible for the fact that drone crashes still happen quite often, mostly during landing, due to the position precision required and the narrow field of vision pilots experience while looking on screen.[84] Other factors may also be relevant for causing drone accidents or even crashes.

The main factors are:

- Suboptimal weather conditions (wind, rain, snow etc.)
- Loss or disruption of data & communication links between drone and remote operator system
- Faults or malfunctions of the machine components[85]
- Human error factors, mostly related to inappropriate handling of the controls[86]

---

80 Will Femia in The Maddow Blog, "Lawnmowers in the dark", November 21st 2012, referring to a BBC publication presenting audio samples of the sound of war, http://maddowblog.msnbc.com/_news/2012/11/21/15343130-lawnmowers-in-the-dark

81 Graham Warwick, "Hovering Near You – IARPA's Quiet UAV"

82 Cf. the article by Jörg Diehl for Spiegel Online of June 22nd 2010, describing the difficulties German police encountered while using drones for certain missions, "Polizei-Drohnen: Himmelfahrtskommando für die Schönwetterspäher", available in German at: http://www.spiegel.de/panorama/polizei-drohnen-himmelfahrtskommando-fuer-die-schoenwetterspaeher-a-701310.html

83 International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at NYU School of Law, "Living under drones: Death, injury, and trauma to civilians from US drone practices in Pakistan", pp. 9 f. (2012), http://livingunderdrones.org/

84 Mark Mazzetti for The New York Times, "The Drone Zone", July 6th 2012, www.nytimes.com/2012/07/08/magazine/the-drone-zone.html?pagewanted=all&_r=0

85 Cf. the blog entry by Matthew Schroyer on DroneJournalism.org of October 27th 2012, describing a drone crash owing to the vehicle's lithium polymer batteries catching fire, "A drone crash in a populated area, and a friendly reminder on drone safety", also showing video footage of the incident: http://www.dronejournalism.org/blog/adronecrashinapopulatedareaandafriendlyreminderondronesafety

86 David Zucchino for the Los Angeles Times, "War zone drone crashes add up", July 6th 2010,

Another drawback of drones is often the lack of encryption during data transmission, making the device vulnerable to hacking by malicious external parties.[87] Already in 2009, U.S. officials admitted that militants in Iraq had been able to intercept video feeds from U.S. Predator drones, using off-the-shelf software.[88] Another hacking attack was also rumoured to have led to the capturing of a U.S. RQ-170 Sentinel drone by Iranian forces in 2011. Such an attack, however, would be very hard to pull off, though experts deem it not impossible.[89] However, Cockrell School researchers from the University of Texas showed that some drones dependent on GPS positioning can be easily misled by conducting a GPS spoofing attack (we also elaborate on this type of attack in Chapter 2.2.4 'Location Trackers', in the subsection 'GPS').[90] Besides proper encryption, another possible countermeasure would be not to rely on GPS only, but also on additional technologies as fall-back procedures in case of malfunction.[91] Generally, it seems that the IT security of the drone operation systems must be improved. Also in 2011, a computer virus infected the cockpits of U.S. Predator and Reaper drones, leading to key logging of pilot control commands during missions.[92] The German department of the ATTAC[93] network warned that while unmanned aerial vehicles appear attractive to governments by providing increased safety for their own ranks through the remote execution of critical missions, the risk of criminals and terrorists getting hold of drones owing to those vulnerabilities and low costs is rapidly increasing.[94]

In relation to data protection, privacy and other civil rights matters, the deployment of unmanned aerial vehicles opens up whole new dimensions of personal surveillance. Especially with regard to future developments of improved capabilities with low flight altitude and little noise, the concerned individuals may not register the covert observation of their person. This stands in contrast to traditional forms of manned aerial surveillance, e. g. by helicopters. Sophisticated equipment like CCTV cameras with powerful zoom and image enhancement capabilities may exist already, but for sure will in near future provide for high quality visual capturing and identification of persons. The visual capture and analysis of crowd behavioural patterns at sports and other public events as well as at demonstrations combined with the identification of individuals standing out of the mass poses a significant threat to freedom of expression and freedom of association in public spaces.[95]

---

http://articles.latimes.com/2010/jul/06/world/la-fg-drone-crashes-20100706

87 Noah Shachtman and David Axe for Wired.com, "Most U.S. Drones Openly Broadcast Secret Video Feeds", October 29th 2012, http://www.wired.com/dangerroom/2012/10/hack-proof-drone/

88 Siobhan Gorman, Yochi J. Dreazen and August Cole, "Insurgents Hack U.S. Drones", December 17th 2009, online.wsj.com/article/SB126102247889095011.html#

89 John Leyden, "Iran spy drone GPS hijack boasts: Rubbish, say experts", whitepaper of December 21st 2011, http://www.theregister.co.uk/2011/12/21/spy_drone_hijack_gps_spoofing_implausible/

90 Cockrell School of Engineering of The University of Texas at Austin, "Cockrell School Researchers Demonstrate First Successful 'Spoofing' of UAVs", http://www.engr.utexas.edu/features/humphreysspoofing; see also the TED video by professor Todd Humphreys elaborating on this demonstration executed by his students: "How to fool a GPS", available at: http://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps.html

91 In 2012, the British armaments manufacturer BAE Systems presented a newly developed navigation system called Navsop (Navigation via Signals of Opportunity) designed for drones, which uses other electro-magnetic waves for positioning besides GPS to provide such a fall-back; for details see the BAE Systems website information: http://www.baesystems.com/home/

92 Noah Shachtman for Wired.com, "Exclusive: Computer Virus Hits U.S. Drone Fleet", June 10th 2011, http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

93 Abbreviation for "Association pour une taxation des transactions financières pour l´aide aux citoyens", roughly translated as "Association for the Taxation of Financial Transactions and Aid to Citizens"

94 ATTAC Germany website entry of June 7th 2012, "Wie Deutschland lernt die Drohne zu lieben", available in German at: http://www.attac-netzwerk.de/cottbus/aktuell/detailansicht/datum/2012/06/07/wie-deutschland-lernt-die-drohne-zu-lieben/

95 Todd Humphreys, professor at the University of Texas at Austin calls this permanent intrusion to citizens' lives "collateral surveillance", see his "Statement on privacy issues related to the domestic use of unmanned aerial vehicles", p. 3, submitted October 25th 2012 in the field forum on privacy issues related to the domestic use of drones, a forum sanctioned by the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security.

But not only are those public spaces spheres of activity for drones. Rather, it is conceivable that a drone is able to fly over private homes and capture video footage of rooms through windows, and of gardens and backyards.[96] The aerial surveillance by the U.S. via balloons over city rooftops in Afghanistan, for example, has attracted particular criticism. Citizens have stated that despite the heat, they cannot sleep on their rooftops as usual anymore, since women and children are exposed to the view of strangers, thus the surveillance is perceived as an *'outrageous intrusion into private lives'*.[97] So, the surveillance from above and from near distance, providing clear images of citizens in their private sphere, can be seen as a severe danger not only to the inviolability of the home, but also to religious freedom. The increasing autonomy of drones, with each improved technological development in that area, takes a step further in the direction of severe legal and ethical issues.[98]

New opportunities for profiling individuals are established by combining an aerial vehicle's video footage with complementary ground-based surveillance technologies like location trackers and conventional CCTV recordings on the ground. This way, detailed movement and contact profiles as well as differentiated behaviour and social profiles become possible.[99] But this raises serious concerns about what impact all these possibilities have on democratic societies compared to authoritarian regimes. Drones would be easily deployable even by otherwise weak authoritarian governments, giving those means to exercise power over their citizens.[100]

Regarding the proposed security-enhancing effects of drones, doubts have been raised from various sides. In particular, the counter-terrorism potential of drones was heavily questioned. Micah Zenko and Douglas Dillon Fellow considered that, in the context of drones, *'Terrorist groups do not disappear owing to military force, no matter how surgical its application. It also overlooks the second-order effects – such as turning public opinion within targeted states.'*[101] This statement is reinforced by the Stanford/NYU report 'Living under drones: Death, injury, and trauma to civilians from US drone practices in Pakistan', which found that the permanent surveillance and casualties of civilians significantly increase the risk that terrorist groups become more successful in recruiting new members.[102] Due to these reasons, there is an urgent need to create sufficient transparency and accountability regarding the use of drones and to closely scrutinise their effectiveness in enhancing security, taking into account the societal impact.

Potential Privacy by Design approaches

Regarding potential Privacy by Design approaches for drones, it must be said that the most significant concerns lie in the advanced equipment such machines may carry. In particular, the features of CCTV provide for a number of possible approaches, which were already described in the previous chapter related to that field of technology. Even so, we refer to the respective chapters below related to the advanced technologies of location trackers and means of communication surveillance. The unmanned aerial vehicles themselves as moving objects have not yet been the focus of discussion in the context of Privacy by Design. Currently, it is suggested to implement privacy rather by organisational measures

---

96 Cf. Thilo Weichert, "Drohnen und Datenschutz – Bedrohungspotenzial und Gesetzgebungsbedarf bei der Beobachtung von oben" (translated: "Drones and data protection – threat potential and need for legislation regarding observation from above"), published in Zeitschrift für Datenschutz (ZD), issue 11/2012, p. 501

97 Graham Bowley for The New York Times, "Spy Balloons Become Part of the Afghanistan Landscape, Stirring Unease", article of May 12th 2012, http://www.nytimes.com/2012/05/13/world/asia/in-afghanistan-spy-balloons-now-part-of-landscape.html?pagewanted=all&_r=0

98 Cf. Chris Cole for Drone Wars UK, "Drone Wars Briefing – Examining the growing threat of unmanned warfare", p. 24, January 2012, www.dronewars.net

99 Weichert, "Drohnen und Datenschutz – Bedrohungspotenzial und Gesetzgebungsbedarf bei der Beobachtung von oben"

100 Cf. author and programmer Daniel Suarez, in an interview with Frank Rieger for the Frankfurter Allgemeine about his recently published book "Kill Decision", publication interview of September 24th 2012, http://www.faz.net/aktuell/feuilleton/debatten/digitales-denken/frank-rieger-interviews-daniel-suarez-swarming-killing-machines-11901656.html

101 Cf. Micah Zenko, Douglas Dillon Fellow, "9/11 Lessons: Unconventional Warfare", Council on Foreign Relations website, http://www.cfr.org/united-states/911-lessons-unconventional-warfare/p25661

102 Stanford/NYU report, pp. 131 ff.

than technical ones, which concern mostly the restriction of drone usage to specific operations under certain legal and factual preconditions.

First steps in this direction have already been taken in the 'Recommended Guidelines for the use of Unmanned "Aircraft"' issued by the International Association of Chiefs of Police Aviation Committee in August 2012.[103] However, it must be noted that these guidelines focus mostly on the general security of drone flight operations and have very few statements regarding legal preconditions and the civil rights of citizens. At least, a judicial warrant for the observation of private property is proposed. Unless exempt by law, public inspection of the drone operation should be enabled. Clear rules for deployment licences should be crafted, and while in use drones should be marked clearly. But none of these recommendations are currently legally binding regulations of unmanned aircraft usage.

Some ideas were delivered by book author Daniel Suarez, who said in an interview that, to provide for some transparency about who uses drones for which purpose, a visual marking of the vehicles is an idea worth supporting. Suarez said that he '*can picture a world where civilian drones are colour-coded by their purpose (e. g. green for city owned, blue for federally owned, red for privately owned) and must display tail numbers – as well as broadcasting a unique ID on some standard frequency. That ID should be able to be keyed into a web registry to determine its owner – and possibly cross-referenced through a Google-maps-like interface to affirm its current location and historical geo-location data. If geo-location is possible on every cell phone, it should be possible with autonomous drones. In such a system, unmarked or incorrectly marked drones flitting about will be immediately suspicious. There might even be city-owned drones charged with spotting unregistered drones.*'[104] However, this proposed solution would not hinder the misuse of drones in relation to the operation in question. Therefore, potential Privacy by Design approaches are yet fairly unknown territory when it comes to drones and provide ample opportunity for future research.

[103] Available as PDF file at: http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf
[104] Ibidem, footnote no. 100

2.2 Network & targeted device surveillance

This section focuses on surveillance-oriented security technologies related to the monitoring of live traffic and data being transmitted through networks as well as on the surveillance of specific static or mobile devices of individuals. Several methods to monitor and filter networks exist, for example HTTP proxy filtering, combined (hybrid) TCP/IP and HTTP proxy filtering, DNS tampering, distributed denial of service (DDOS) attacks, and also Internet domain registration and server take downs. However, since a full description of all these possibilities is not possible within the scope and time frame of the SurPRISE project, we focus on four relevant categories: The first subsequent section will present Deep Packet Inspection (DPI) as a method of Internet surveillance (Chapter 2.2.1), while the following section focuses on components used for the content surveillance of specifically targeted devices, e. g. by Trojan Horses as part of a complete bundled surveillance system (Chapter 2.2.22.2.3). Moreover the surveillance of households by means of smart meter surveillance (Chapter 2.2.3) and the tracking of individuals by usage of location trackers for mobile devices (Chapter 2.2.4) will be described.

2.2.1 Deep Packet Inspection for Internet surveillance

Internet surveillance means the monitoring of data and traffic on the Internet. As the Internet is arguably the most important communication channel, governments globally perceive this medium as a danger to security as well as a chance to obtain information useful in preventing and investigating security threats and incidents. Looking for direct access to information, governmental agencies worldwide turn mainly to the providers of broadband Internet connection and Voice-over-Internet-Protocol (VoIP) services. Seeking to oblige these providers to employ their own infrastructure capacities to constantly monitor, screen, analyse and filter data traffic, high hopes are set on this approach to identify terrorists and other criminals.

For example, in the United States, the extension of the Communications Assistance for Law Enforcement Act (CALEA) now foresees an obligation of communications intermediaries to routinely intercept phone calls and broadband Internet traffic (e-mails, web traffic, instant messaging etc.). Also, privacy functionalities will require a backdoor and the use of encryption is restricted.[105] In the United Kingdom, the government also expressed the desire to implement new regulation extending the surveillance of e-mail and social media communications, sparking a heated debate about the necessity and proportionality of such measures.[106] In Germany, the surveillance of e-mail communication has increased significantly since 2009. In 2010, German intelligence services inspected 37,292,862 e-mails and data connections, a number quintupled from 2009, when 6.8 million Internet and other network communications were inspected. Over 15,300 key words related to the topics of terrorism, proliferation, immigrant smuggling and trafficking were used to filter e-mails, but only led to actually useful clues in 213 investigation cases.[107]

In this chapter, we will present these forms of Internet surveillance as a broad concept to monitor or screen communication routed through a network node. Though social media providers such as Google, Facebook etc. may have the ability to implement DPI into their own systems to surveil the content uploaded to their servers and give access to security agencies, we will hereinafter solely focus on DPI established throughout the open network/Internet by ISPs. Typically, the vast amounts of data intercepted and automated means for correlating filtering mean that the individual-case monitoring by

[105] Federal Communications Commission News Media Information letter of August 5th 2005, titled "FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps", https://w2.eff.org/Privacy/Surveillance/CALEA/FCC_voip_wiretaps.pdf, and Seth Schoen, Electronic Frontier Foundation (EFF), "Legal Struggles Over Interception Rules in the United States", https://www.eff.org/pages/legal-struggles-over-interception-rules-united-states

[106] Robert Booth in The Guardian, "Government plans increased email and social network surveillance", April 1st 2012, http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance

[107] ZEIT Online, "Mail-Überwachung durch Geheimdienste deutlich gestiegen", published February 25th 2012, http://www.zeit.de/digital/datenschutz/2012-02/geheimdienst-ueberwachung-email

human personnel has long since been replaced. Pre-defined filtering algorithms allow for a fine-grained alert system, including the use of certain words or phrases in communication channels like e-mail, VoIP or chat, the visit of certain web sites, or the communication with a specific individual or group. These preceding examples make apparent that the conventional scenarios of Internet surveillance closely relate to two main aspects of Internet communication: e-mail and social network content. The core technology to achieve the surveillance of these means of communication between citizens is the deployment of Deep Packet Inspection technology, allowing for an extensive monitoring and analysis of data packets being sent via the Internet. Internet service providers can deploy DPI within their own infrastructures to scan the traffic being routed via their servers, e. g. to achieve:

- Network stability
- Network/Bandwidth management
- Content filtering, spam detection, and blocking of websites
- Rerouting e. g. to own search sites in case a website is not directly accessible
- Profiling for targeted advertising
- Manipulation of websites for more efficient transmission
- Provision of governmental surveillance and censoring infrastructures[108]
- Blocking of encryption and tunnelling systems preventing lawful interception[109]

Considering this extensive list, it becomes clear that the motivation of ISPs in using DPI for monitoring user data being sent over their network infrastructures can have a quite wide scope. From their point of view, DPI may seem necessary to provide their core services properly even though this might not always be the case.[110]

State of technology

Deep Packet Inspection (DPI) is a technology which can be used to extract user data which is sent between different devices via networks. Depending on the concrete design and deployment of the DPI technology, it is possible to perform the surveillance measure on a broad scope via the respective Internet Service Provider (ISP). Each communication over networks, such as the Internet, occurs in form to a transmission of data packets over an electronic network. To understand the difference between DPI and other means of packet inspection, it is important to know that each data packet that is sent between devices consists of several layers defining protocols and functionalities of the packet. To enable the reader to further understand the implications, Figure 1 visualises the different layers according to their definition in the ISO/IEC 7498-1 standard.

---

[108] Christian Fuchs, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", pp. 9 ff., entailing a detailed description of the technological approaches to achieve these purposes.

[109] Klaus Mochalski, Hendrik Schulze, "Deep Packet Inspection – Technology, Applications & Net Neutrality", page 6, white paper published 2009 for the company ipoque, a provider of DPI technology for Internet traffic management and analysis, available as PDF file at: http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

[110] Cf. Ben Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control, pp. 6 f.; moreover, especially the network stability reasons for the deployment of DPI by ISPs are also mentioned in the recently developed standard issued by the International Telecommunication Union (ITU), now known as "ITU-T Y.2770, Requirements for Deep Packet Inspection in Next Generation Networks"

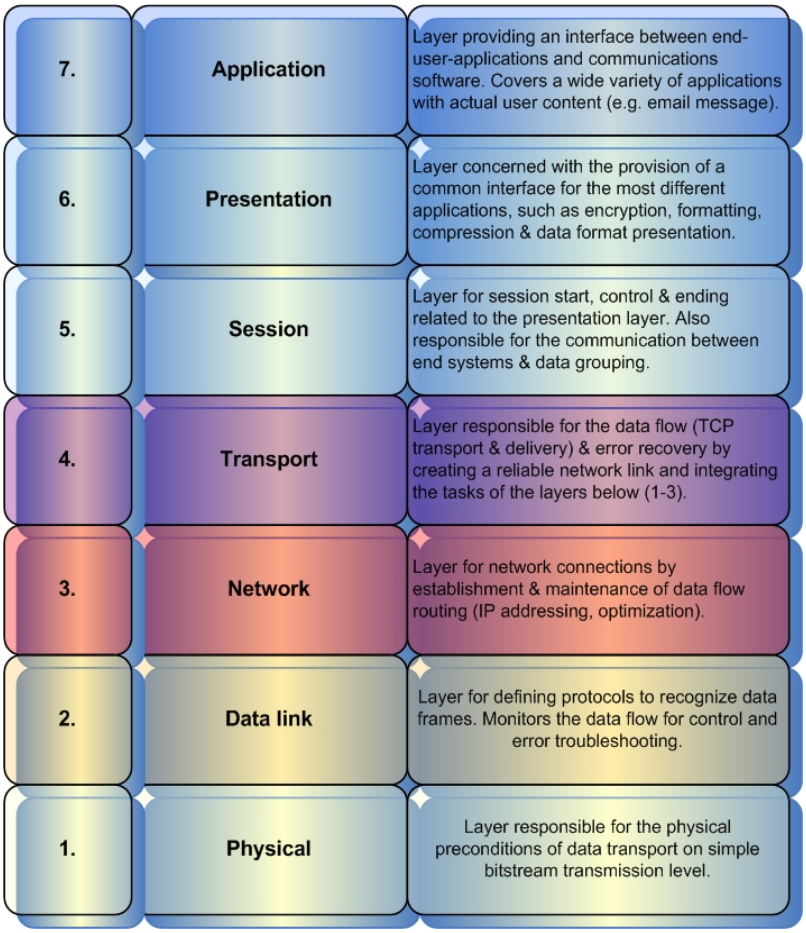

Figure 1: The Open Systems Interconnection (OSI) model

Each layer includes a header and subsequent data (payload) related to its respective functionalities. The user data (e. g. the content of an e-mail message) is included on the uppermost level 7 (see Table 1).

Payload	**TCP Header**	**IP Header**
Application data: e-mail text, URL, Website content, chat message, video content, image content etc. Application header: application programme version, e-mail address sender/receiver etc.	Source port Destination port Sequence number	Source IP Destination IP Total length
Defined at TCP/IP layer 5 (OSI layers 5, 6, 7)	Defined at TCP/IP layer 4	Defined at TCP/IP layer 3

Table 1: A TCP/IP packet[111]

To understand what DPI exactly does, it may be useful to look at other forms of packet inspection to highlight the differences. For example, to provide its Internet connection service, an ISP theoretically just needs to inspect the headers of the layers to obtain information from which device the data packet

[111] Source: Christian Fuchs, "Implications of Deep Packet Inspection (DPI) Internet Surveillance", 2009

is sent and which destination it has. Hence, the provider performs a 'Shallow Packet Inspection' whereby he does not need to learn the content of each packet. Consequently, this form of packet inspection mainly focuses on an analysis of the TCP headers on layer 4, respectively on the IP headers on level 3 to obtain knowledge of the open ports of a device and to ensure network connection and stability. A slightly more intrusive form would be the so-called 'Stateful Packet Inspection', whereby not only the headers but also the payload of the layers 3 and 4 are analysed. In this context, it is important to know that each layer contains fragmented information of the above layer. So if the fragmented parts can be composed together, the packet inspecting system would be able to derive content/payload information of the upper layers as well. An example is shown in Figure 2, where it is visualised how a combination of fragmented layer 3 and 4 parts leads to the obtainment of level 5 (session layer) content, which reveals information about the website the targeted individual visited, using his or her personal device.

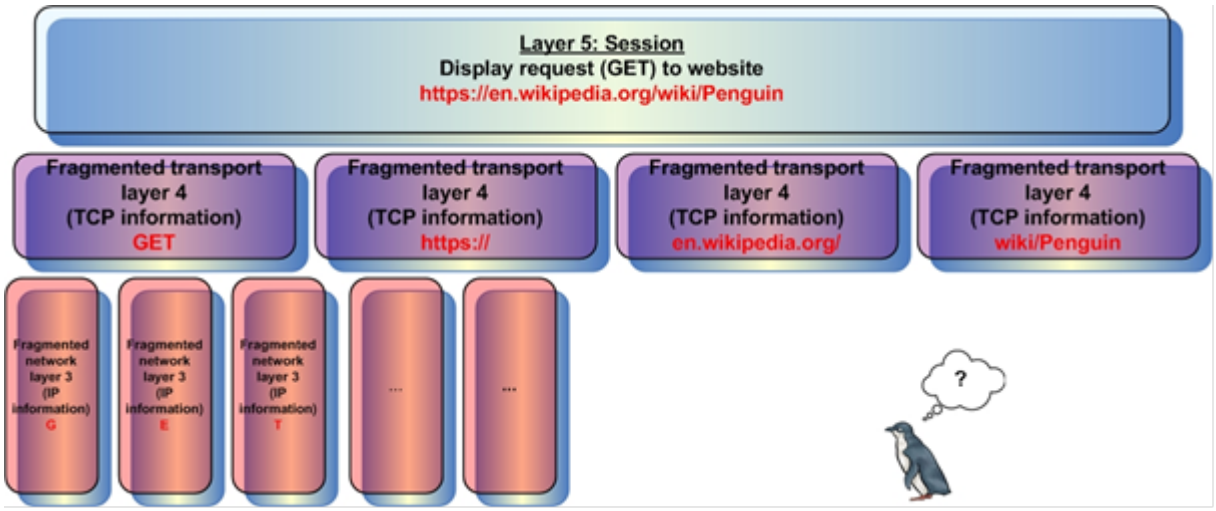

Figure 2: Layer fragmentation (simplified model)

However, in contrast to these aforementioned possibilities, DPI directly focuses on all seven layers and not just their headers. In doing so, it is able to recognise a variety of information bits contained in headers and payload of each data packets. Recognisable for DPI systems are:

- Protocols
- Applications
- URLs (Internet addresses)
- Media content (specific instances of recorded music, movies, images or books)
- Text strings
- Data with a specific format (e. g. credit card numbers, Social Security Numbers)[112]

So it becomes apparent that the DPI system is aimed at a full analysis of user data included in all 7 levels of the packet, as shown in Figure 3.[113]

[112] Cf. Milton Mueller, Syracuse University School of Information Studies, "DPI Technology from the standpoint of Internet governance studies: An introduction", pp. 2 f., October 21st 2011, http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf

[113] Mark Bedner, "Rechtmäßigkeit der Deep Packet Inspection" (translated: "Lawfulness of the Deep Packet Inspection"), page 6 f., analysis created for the "Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" at the Universität Kassel, published 2009 and available in German at: kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf

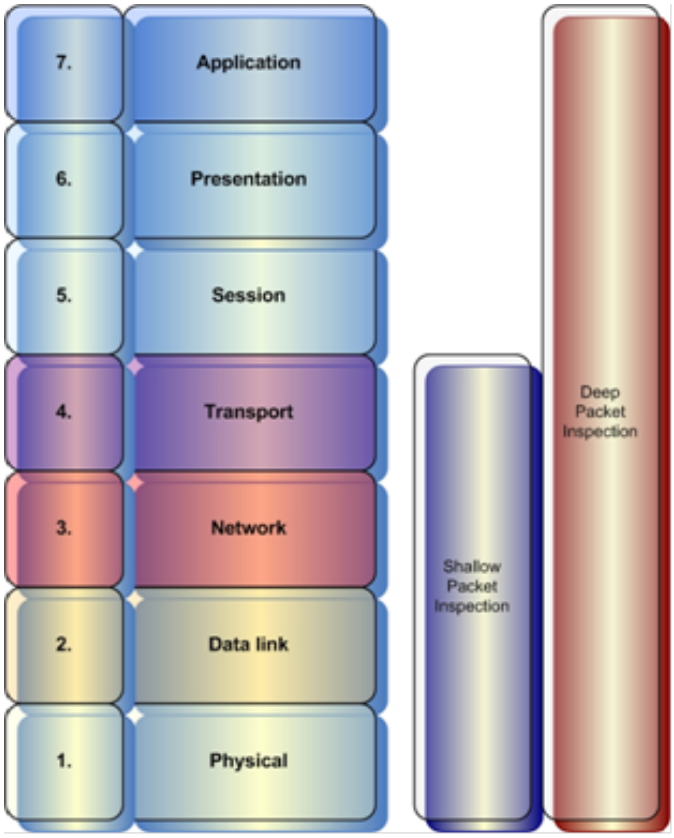

Figure 3: Different depth of SPI and DPI

So DPI can be seen as the most all-embracing method of data packet inspection, leading to a comprehensive surveillance of data transmissions between devices. This technology is able to analyse headers as well as payloads of each layer of the packet. Thus, this technology is well equipped to learn the content of the communication between two users. The lower layers 1-4 contain crucial information for Internet Service Providers to deliver their Internet connectivity services. As explained, ISPs do not usually necessarily need to perform the more intrusive forms of packet inspection above layer 4 since the relevant information for providing the Internet services is contained in the TCP and IP layers. Still, using DPI technology is sometimes convenient for ISPs owing to a variety of reasons, from network stability to content filtering purposes.[114] In the following sections, we will shortly describe means of Internet surveillance based on the two classic scenarios: e-mail and social network communication surveillance.

➢ *E-mail surveillance*

Whenever communication data is sent over the Internet, it is routed to and received at its final destination. During this process, network surveillance tools may screen each data packet passing through and perform pre-defined additional actions, such as filtering or altering content. The screening could mean anything from a passing browse to Deep Packet Inspection – depending on the tools used and the set-up. Theoretically, this can happen at each and every web server or network node the data packet is routed through. Simply put, it is necessary to run additional surveillance software on the hardware of the network. Such hardware would be the servers of the respective ISPs being obliged by

[114] Christian Fuchs, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", p. 15, created for The Privacy & Security Research Paper Series issue #1 and published in July 2012, http://www.projectpact.eu/documents-1/%231_Privacy_and_Security_Research_Paper_Series.pdf

security agencies to execute the monitoring of data packets (see Figure 4). Whenever two users of the Internet send e-mails to each other, data packets are sent and received from their devices, containing information needed for the determination of their route through the Internet, crossing the servers of the respective Internet Providers of the users. In reference to the OSI model shown in Chapter 2.2.1 (see Figure 1), Internet routers need the IP information contained in layer 3 to send data packets onwards to their defined final destination. Beyond the IP of a destination computer or other network-connected device, the TCP-information on layer 4 is important for firewall systems to extract the transport protocol (such as TCP or UDP) and IP port number (which is commonly associated with a specific application; e. g. port 80 for web services).[115]

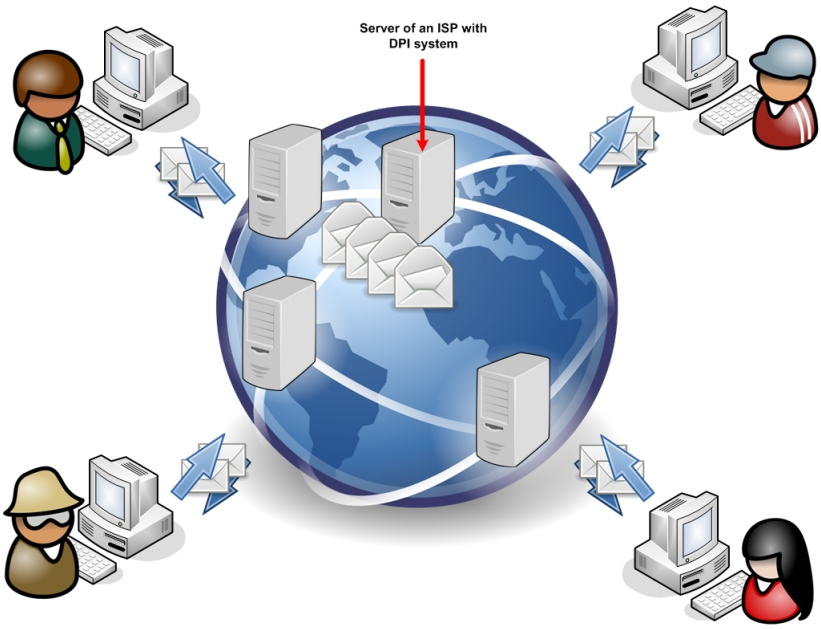

Figure 4: Internet data packet interception

As already explained and visualised above (see Figure 3), Deep Packet Inspection (DPI) goes much further and is able to analyse all layers of the packet. It is focused on an analysis of data packets in motion (i. e. on their way to their destination). Thus, a deployment of DPI not being installed covertly on a single device belonging to a specifically targeted individual is basically to be seen as an application on a server to detect and further handle live traffic on a network like the Internet.[116] Depending on a pre-defined pattern or filtering instruction, the analysis of high-speed Internet data transmission requires highly advanced hardware and algorithms. So the deployment of effective pattern-matching algorithms can be highly resource-intensive. Moreover, these pattern-recognising algorithms must be constantly updated and expanded to function adequately over a longer time span. This requires constant management of the DPI system, sometimes called a DPI Engine.[117] Beyond the screening of live traffic, DPI is able to perform the manipulation of data packets according to a prior instruction (so-called active parameter instead of just passive screening). Several forms of manipulation are possible, such as:

- Block the movement of recognised informational objects into or out of the network
- Regulate (rate-limit) packet flow speed
- Change the packet header in some way

[115] Sean Gallagher, arstechnica.com article of September 27th 2012, "Big Brother on a budget: How Internet surveillance got so cheap", http://arstechnica.com/information-technology/2012/09/big-brother-meets-big-data-the-next-wave-in-net-surveillance-tech/

[116] Milton Mueller, "DPI Technology from the standpoint of Internet governance studies: An introduction", pp. 1 f.

[117] Ibidem, pp. 3 ff.

- Prioritise (or deprioritise) some protocol's packets over others
- Prioritise (or deprioritise) some user's or class of users' packets over others
- Disconnect a session

Considering the above-mentioned possibilities for conducting manipulations of data packets, the alteration of e-mail message content is basically a matter of prior configuration and defined commands to the DPI system. Furthermore, in case of a matching pattern according to the used algorithm, notifications or alarms may be issued to the administrators in charge of the DPI Engine management. Depending on the configuration of the DPI system, the monitoring and possibly manipulation of data packets may be realised in two ways. The first possibility is to deploy the monitoring application in a position directly located in the traffic stream (so-called in-line DPI), which is generally more fit for on-the-fly manipulation procedures transparent to the users. The second possibility is an off-line deployment, which diverts a copy of the data packet traffic to the DPI Engine and can be used to perform notifications to the administrators.[118] The latter option would then also be fit for the interception of e-mail traffic to or from a specific user performed by the ISP by request of security agencies. Whichever approach is chosen, the ISP could reroute the traffic to an encrypted IPsec VPN gateway installed to enable security agencies to have direct access to the e-mail messages from there.[119]

➢ *Social network surveillance*

After the devastating events of 9/11, security agencies worldwide focused on combatting terrorism. They realised how terrorists became acquainted with each other for organising their undertakings, and Internet communication – in particular of social media that have flourished several years later– caught their attention, leading to new approaches in understanding and analysing communication conducted using social media channels. Since then, innovative technological approaches have been increasingly demanded as a countermeasure for aiding crime prevention as well as crime investigation in many parts of the world, including the European Union. In a recent course of events, the technical committee of the European Telecommunication Standards Institute (ETSI) published a draft document presenting new technical standards on how to provide real-time access for security agencies to cloud services and social networks. Regardless of location, providers of services like Facebook, Google+, LinkedIn, Amazon, Twitter and Microsoft would be concerned by these new standards. According to this document, the service providers would be obliged to implement backdoors, including an alert system for encrypted data packets.[120] It remains to be seen whether these standards will become mandatory for the ISPs for implementation.

The current state of the art in social network surveillance combines the techniques of the above-described DPI network monitoring with new technologies of data mining. In doing so, filtering algorithms are tuned in for atypical behavioural patterns and the automated removal of inappropriate and illegal content. But the effectiveness regarding security enhancement in social networks remains doubtful since the predefinition of atypical user behaviour does not always lead to satisfying results.[121] Still, automated procedures to monitor online content are often used to filter and censor data uploaded and hosted in social networks, an approach increasingly used to combat child pornography and copyright violations, i. e. illegal file sharing.[122]

---

[118] Ibidem, pp. 4 ff.

[119] Cf. National Institute of Standards and Technology (NIST), special publication 800-77, "Guide to IPsec VPNs", p. A-4

[120] Cf. the details in the ETSI DTR 101 567 V0.0.5 draft technical report of March 2012, available online as Word file at: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_LI/2012_45_Bratislava/SA3LI12_044.doc

[121] Joseph Menn, "Social networks scan for sexual predators, with uneven results", published July 12th 2012, http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712

[122] Christian Fuchs, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", p. 25

➢ *Other means of Internet surveillance*

Since 2003, the OpenNet Initiative has been conducting an on-going documentation of Internet filtering to find out in how many states worldwide Internet surveillance is practised, resulting in the filtering of online content. The documentation revealed that of 74 countries tested worldwide, 42 states censored network traffic,[123] most of them blocking content from being accessed by their citizens. Apart from physically removing the content servers, filtering content may also be executed using DPI on backbone nodes of the network. Alternative options worth mentioning briefly are the blacklisting of IP addresses, DNS spoofing (preventing communication with certain domains), or the redirection of the user to another web server.[124] However, all of these means of filtering are also possible complementary actions to DPI interception of data-driven communication, for example the 'GET' request to a website for displaying its content (cf. Figure 2). This sort of surveillance may be even more effective in not only denying the user access to certain online content, but also in monitoring his or her information requests and web-surfing behaviour.

Effectiveness of Internet surveillance and civil rights impact

There is little to no data on how effective the above-described Internet surveillance technologies are with regard to preventing and investigating terrorist and other criminal activities on the Internet. Conducted review attempts remain most often politically influenced or too vague to present useful results for current research for security enhancement. Taking into account the vast technical possibilities, it seems that at this time, only the resource intensity and costs set limitations on the deployment of such technologies. But upcoming developments in the field of Big Data analysis lead to a persistently growing cost-efficiency. So it may be reasonable to believe this will spark the interest of security agencies to fully embrace highly intrusive security measures like the ones which were presented in this chapter. But such measures also come with significant negative impact on citizen rights. In particular, DPI technology – which is able to monitor, filter, analyse, store away and manipulate all kinds of digital citizen data – has high potential to be misused for social discrimination, political repression, censorship and serious infringement on sensitive areas of private life.[125] Whatever the intention of such measures, the risk of over-enforcement is significant owing to their highly intrusive nature and legislative measures always being a step behind the technological possibilities.[126]

Potential Privacy by Design approaches

Owing to their aforementioned attributes, Internet surveillance technologies provide depending on their case-specific configurations high potential of negative civil rights impact and privacy intrusion. Thus, the realisation of Privacy by Design in this field is to be seen as nearly impossible at this stage. At least potential limitations of DPI are being discussed for privacy risk mitigation, e. g. limiting the depth, breadth and data retention which is possible for some use cases, and ways to notify users. [127] If not addressing the technology itself, the surrounding can be put into focus where privacy by design may be affected: From the perspective of national security of a state it may make sense to protect the communication of its own citizens against DPI from foreign countries. This encompasses both governmental communication and Internet usage that may be prone to industrial espionage. So a state may have an interest to protect these kinds of communication against other countries by end-to-end encryption, anonymising technologies and constrained routing of Internet packets from citizens that

---

123 TheOpenNet Initiative website entry of April 3rd 2012, "Global Internet filtering in 2012 at a glance", available at: http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance

124 TheOpenNet Initiative website information, "About filtering", http://opennet.net/about-filtering

125 Cf. Ben Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control", pp. 2 f.; Christian Fuchs, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", p. 25

126 Cf. Hiram A. Meléndez-Juarbe, University of Puerto Rico Law School, "Intermediaries and Freedom of Expression", pp. 1 f., essay translated by University students Edgardo Canales and Marini Rodriguez, available at: http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/04-Intermediaries_Freedom_of_Expression_Hiram_Melendez_Juarbe.pdf; also cf. Mark Bedner, "Rechtmäßigkeit der Deep Packet Inspection", p. 34

127 Alissa Cooper, "Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection", in: William Aspray, Philip Doty (Eds.), Privacy in America: Interdisciplinary Perspectives, 2011, p. 160

stays as far as possible within the realm of the own country or other countries where a misuse by ISPs or the government seems to be unlikely. While this is clearly not a solution for global Internet communication, it may make sense for domestic communication. A state may also issue warnings concerning probable or proven surveillance of other countries. This at least would raise awareness among users.

Summarising, DPI technologies appear as a severe danger to democratic core principles in protecting the fundamental rights of European citizens. So at this current stage, it is advisable to closely monitor future technical developments in this area and restrict the usage of DPI to prevent a more widespread usage until the technical and legal grounds of its deployment are sufficiently and unambiguously defined.

2.2.2 Content surveillance on targeted devices

From the viewpoint of security agencies, the surveillance of citizens' telecommunication is a key tool to enable effective crime prevention as well as crime investigation. The conventional methods of telecommunication surveillance enable the direct extraction of data during a running telecommunication process. However, during Internet-based telecommunication, these methods are often not sufficient for their usual purpose. This is owing to the fact that typically the telecommunication providers are not able to ensure the extraction of unencrypted data, whereas de-ciphering encrypted data is usually difficult at best. Consequently, telecommunication surveillance can be achieved by collecting and deriving the data directly from the device of the targeted individual before the encryption process occurs, or, alternatively, when it gets unencrypted. In these cases, technology for network communication and data packet inspection are brought onto the individual devices by means of Trojan Horses, and thereby creating a backdoor to the system. This opens up the possibility of effective communication interception. Also, beyond the mere interception of telecommunication, it possibly enables further means of surveillance, for example by being accompanied by additional malware, as we will describe below. These may go far beyond mere wiretapping of Internet telephony up to complete online searches of targeted devices.

However, owing to its potential, this technology poses a severe threat of misuse for comprehensive surveillance of citizens in Europe and beyond. For example, in August 2011, the French company Amesys provided Deep Packet Inspection technology to Gaddafi's regime in Libya, where it was used to spy on political opponents.[128] For this, two human rights organisations, the International Federation for Human Rights (Fédération internationale des ligues des droits de l'Homme – FIDH) and the Human Rights League of France (Ligue des Droits de l'Homme – LDH), filed criminal charges against the company. In January, the Paris Court of Appeal allowed the resulting judicial investigation to continue.[129] Other companies have faced similar charges, like the British firm Gamma International whose FinSpy software from their FinFisher product portfolio was used against political opponents and activists in Egypt and Bahrain.[130] The company Blackshades sold a commercial Trojan to the Syrian government, which used it against activists by performing key logging, taking remote screenshots, obtaining log-in credentials of website accounts and installing malware.[131] Even more cases of

[128] Paul Sonne and Margaret Coker, The Wall Street Journal Online, "Firms aided Libyan spies – First Look Inside Security Unit Shows How Citizens Were Tracked", August 30th 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html#

[129] Fidh online press releases of October 19th 2011, "FIDH and LDH file a complaint concerning the responsibility of the company AMESYS in relation to acts of torture", http://www.fidh.org/FIDH-and-LDH-file-a-complaint, and of January 17th 2012, "Amesys Case: The Investigation Chamber green lights the investigative proceedings on the sale of surveillance equipment by Amesys to the Khadafi regime", www.fidh.org/Amesys-File-The-Investigation-12752

[130] Bloomberg.com article by Vernon Silver, July 25th 2012, "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma", http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html

[131] EFF article by Eva Galperin and Morgan Marquis-Boire, July 12th 2012, "New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan", https://www.eff.org/deeplinks/2012/07/new-blackshades-malware

surveillance technology distribution were disclosed in December 2011 by the release of the so-called Wikileaks Spyfiles.[132]

But such technologies are not just used in countries outside Europe. The so-called German State Trojan was first made known, reverse engineered and analysed by the German Chaos Computer Club in October 2011.[133] Another version of the Trojan was further analysed shortly after, revealing even more functionalities the Trojan can perform on the targeted device.[134] However, the legality of such surveillance methods was questioned, leading to several investigations of supervisory authorities.[135] In the United Kingdom, legislative efforts were initiated in June 2012 by publishing a draft of a new Communications Bill, which would significantly widen the powers of governmental agencies regarding the surveillance of digital communication. Still, the draft remained unclear on which measures exactly will be legalised under the future law, triggering much criticism from privacy and human rights organisations fearing the start of an all-embracing mass-surveillance of UK citizens.[136]

State of technology

The infiltration of a specifically targeted device in contrast to wide-range Internet surveillance occurs through software which was brought onto the personal system. This software, most often a Trojan Horse, functions covertly, without revealing its real functionalities to the user of the device. In fact, it may also be complemented by DPI technology as a remote tool to capture the telecommunication data before it gets encrypted to leave the device on its transmission route. Then the network capabilities of the specific device are used to transmit its obtained data as a sending entity to a receiving entity, where it is directly accessible for the executing governmental agencies.[137] This receiving entity in turn sends commands to the sending entity to initiate or control specific operational functionalities (see Figure 5). The exchange between both entities usually occurs over one or several proxy servers to disguise the route of the connection.[138]

---

132 http://wikileaks.org/the-spyfiles.html

133 Chaos Computer Club Blog entry, "Chaos Computer Club analyzes government malware", published October 8th 2011, http://www.ccc.de/en/updates/2011/staatstrojaner

134 Chaos Computer Club Blog entry, "Chaos Computer Club analyzes new German government spyware", October 26th 2011, http://www.ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner

135 As for an example, the Bavarian Data Protection Commissioner scrutinized the deployment of the malware in the Federal State Bavaria and questioned the lawfulness of its usage in his report "Prüfbericht Quellen-TKÜ", published July 30th 2012. The full report is available in German at http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf

136 Privacy International, June 15th 2012, "Draft Communications Bill reveals Home Office's mass surveillance plans going ahead – but government remains tongue-tied about how technology will actually work", https://www.privacyinternational.org/press-releases/draft-communications-bill-reveals-home-offices-mass-surveillance-plans-going-ahead

137 For the German "State Trojan" this software is named "Remote Capture Unit" which is brought onto the device itself. Its counterpart, the remote receiving station, is named "Recording Unit". See the investigation report of the Bavarian Data Protection Commissioner: "Prüfbericht Quellen-TKÜ", July 30th 2012, pp. 17 ff.: http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf

138 Ibidem, pp. 17 ff.

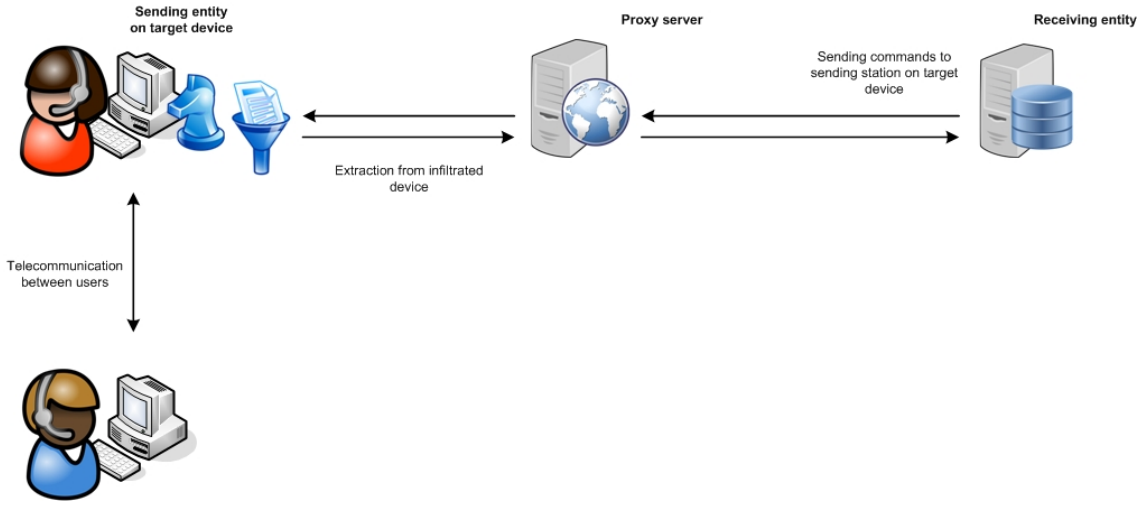

Figure 5: Extraction of data from infiltrated device

The Trojan is usually brought onto the device covertly. This can occur in different ways: for example, the visit of a prepared website link (drive-by download) or the opening of an e-mail attachment may trigger the installation. Other possibilities are the usage of so-called infection proxies or direct physical access to the device.[139]

The often specifically tailored surveillance solution enables the installation and launch of programs with a diversity of different functionalities. So for example, the so-called German State Trojan, analysed by the German Chaos Computer Club (CCC), was criticised for its intrusive potential in relation to the functions possible. According to the CCC, the remotely controlled Trojan is able to integrate backdoor functionalities for uploading and executing a multitude of arbitrary programs, thus giving it full remote control over the infected device via its update function. The used Trojan combined with the DPI technology went far beyond the needed programs for wiretapping Internet telephony and provided e. g. screenshots, audio recording and manipulation of allegedly 'revision-proof logging'.[140]

The FinFisher spyware of the Gamma group mentioned in the introduction could be used to record Skype calls and chats, to monitor the device user via webcam and microphone and to perform key-logging operations, thus learning everything that is being typed on the keyboard, especially passwords.[141] According to the Wikileaks Spyfiles, the FinSpy technology was advertised by the vendor with possible functionalities such as bypassing 40 regularly tested antivirus systems, covert communication to the receiving entity, Skype monitoring (calls, chats, file transfers, video, contact list), e-mail, chat and VoIP recording, live surveillance through webcam and microphone, country tracing of target device, extraction of hard-disk files, key logging, remote forensics and data filters. The technology was further promoted as supporting the most common operating systems, Windows, Mac OSX and Linux.[142] Moreover, recent news indicated that the FinFisher spyware features new versions designed for mobile devices and executing e. g. silent calls, country tracing of target devices through GPS and cell ID

---

139 These are the possibilities assumed in the first analysis conducted by the German Chaos Computer Club, titled "Analyse einer Regierungs-Malware" (translated: "Analysis of a state malware"), p. 3, October 8th 2011, http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (German version CCC report with link to the government trojan's binaries)

140 Chaos Computer Club Blog entries, summarising the findings of the analyses: "Chaos Computer Club analyzes government malware" of October 8th 2010 & "Chaos Computer Club analyzes new German government spyware" of October 26th 2010

141 Vernon Silver at Bloomberg.com, "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma"

142 The Wikileaks Spyfiles, document #289, "Remote Monitoring & Infection Solutions: FINSPY", http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf

information, address book data exfiltration, call interception, phone call log extraction and recording of incoming/outgoing SMS.[143]

In July 2012, a Trojan spyware for smartphones called Crisis or Morcut was discovered, and is assumed to be a later version of the remote control system Da Vinci created by an Italian company. This Trojan is able to run on different operating systems like Windows and Mac OS. It also provides a number of functionalities ranging from Skype monitoring, key logging, and webcam recording up to the infection of Virtual Machines (VMs). Moreover, a remote application programming interface enables the installation of additional modules. The original Da Vinci Trojan was known to also function under iOS, Android, Blackberry, Symbian and Linux systems.[144]

Summarising the capabilities of the above-mentioned examples of such systems, the technology is, depending on the individual configuration, able to provide the following functionalities:

- Compatibility with different operating systems
- Monitoring systems (Internet telephony interception, chat logging, file transfers)
- Application monitoring/screenshots
- Application filters
- VoIP telecommunication surveillance
- Listing of installed software
- Country tracking of the infected device, also on mobile devices via GPS and cell ID
- Address book/contact list data exfiltration
- Execution of programs and processes
- Inducing system crashes ('blue screen') or re-booting of device
- Updates of sending station software on device
- Key logging
- Activation of cameras & microphones
- Manipulation of data
- Deinstallation

This list is not to be seen as conclusive since the built-in update function of most surveillance solutions allows for later installation of additional functionalities including remotely controlled searches on the whole target system (all-embracing online search). Also thinkable is the manipulation of inbuilt speech and facial recognition applications to identify individuals using the device. The update process itself is fairly simple: the receiving entity for the remote control transmits the new binary files to its counterpart entity on the infiltrated device. This process can theoretically be started each time the sending entity on the device obtains access to an Internet connection.[145] Consequently, the Trojan is in its design right from the beginning open enough to integrate further means of infiltration and surveillance, using the

[143] Morgan Marquis-Boire, Bill Marczak, "The SmartPhone Who Loved Me: FinFisher Goes Mobile", pp. 1 ff., 25; The Citizen Lab at the University of Toronto, Research Brief Number 11, published August 2012, https://citizenlab.org/wp-content/uploads/2012/08/11-2012-thesmartphonewholovedme.pdf

[144] The H Security Blog entry, published August 22nd 2012, titled "Multi-platform spyware penetrates smartphones and VMs", available at: http://www.h-online.com/security/news/item/Multi-platform-spyware-penetrates-smartphones-and-VMs-1672259.html

[145] Cf. the findings in the investigation report of the Bavarian Data Protection Commissioner: "Prüfbericht Quellen-TKÜ", p. 32 (in German).

device of the targeted individual. So while the current state-of-the-art DPI technology is already widely criticised in public as being over-intrusive, yet unknown future technological developments will prove to be uncharted areas regarding benefits and drawbacks in the context of a security and privacy trade-off matters.

Effectiveness of content surveillance on targeted devices and its civil rights impact

The selection and targeting of the intended device without failure is the most crucial precondition to achieving the purpose of the measure. Consequently, it is important to make sure the Trojan is brought onto the correct device. Usually, security agencies already have used prior standard telecommunication and Internet surveillance methods to get an impression of the installed programs and configurations of the target device to distinguish it from other devices.[146] What all of the above-mentioned surveillance systems have in common is an inbuilt update function which can be activated once the infected device is connected to the Internet. This function enables the later installation of other functionalities and upgrades, making it easier to remedy malfunctions and shortcomings of the software. This of course requires the Internet connectivity of the infected device to enable the contact between the entity components of the system. Still, the Trojan needs some fixed preconditions to function properly.

Moreover, a deinstallation function is mandatory to ensure that the surveillance measure is limited to a pre-defined time frame. Not later than after the expiry of the period in which the surveillance of the individual is meant to happen, the Trojan shall be deactivated and deleted from the infected personal device. However, the fulfilment of this requirement can prove problematic under certain circumstances. In cases where no physical access to the device is guaranteed, the deinstallation process needs to be triggered via the remote control entity. But this procedure can only occur if the device connects itself to the Internet so a contact between the sending and receiving entities is possible. Besides the Internet connectivity of the infected device, the involved proxy server(s) must still be active and accessible. So in case the receiving entity tries to connect to the sending entity after a proxy server was deactivated or its IP address was changed, the contact is not possible. Furthermore, there is a danger that the complete Trojan gets re-activated if system backups from the infected device were made and get re-installed. All of these factors mean that a deinstallation might not be possible at each time but only limited to those prerequisites. To avoid such dependence, it is advisable to pre-define a set time frame for deinstallation directly in the code of the sending entity component on the device.[147]

As for the communication between the entities, the encryption must adhere to the newest security standards to protect the data against unauthorised third-party access. In Germany, the CCC heavily criticised the fact that the deployed technology did not follow the basic cryptographic standards, thus exposing the data of the targeted persons to malicious exploitation from third parties. Also, they stated that the infiltration of the system makes it in general more vulnerable to attacks from malicious third parties. In this context, the CCC did not rule out the possibility that even the IT infrastructures of the security agencies may be attacked via the receiving remote control entity owing to insufficient authorisation of the single entities to each other.[148] In the context of authorisation to the system, it must also be ensured that within the security agency, only authorised persons can access and control the receiving entity. Such a limitation could only be safeguarded by effective access controls on technical and organisational level. Also, to make such an access control verifiable, any access to the system should be logged sufficiently and securely, aligned with the relevant legal requirements.[149]

Besides these security aspects of this surveillance solution, the limitation of the measure to the extent needed and legally compliant in context of the intended purpose proves as the most crucial criticism point. Even if a later update possibility is not used, some inbuilt functions of the Trojan Horse used to

---

[146] Ibidem, pp. 21 f.
[147] Ibidem, pp. 32 f.
[148] See the CCC State Trojan report "Analyse einer Regierungs-Malware" in German, p. 2, and the related CCC Blog entry, "Chaos Computer Club analyzes new German government spyware"
[149] The Bavarian Data Protection Commissioner: "Prüfbericht Quellen-TKÜ", pp. 42 ff.

bring additional malware such as DPI onto the system may unintentionally goes beyond the scope allowed for the venture. So for example, it cannot be guaranteed that application/screenshot functions don't capture data going far beyond mere telecommunication surveillance instead of everything the user of the device does with the system. Thus, the implications regarding data protection and human rights must be seen on a wide spectrum of potential impact issues. At this point, we will highlight some of the most urgent issues mostly relevant to the personal device surveillance aspects of such highly advanced surveillance systems.

As described above, the possibilities regarding configuration and functions of these complete systems currently used are practically endless. These possibilities are even more difficult to ascertain since the initially inbuilt update function enables a later installation of additional features as an add-on to the existing system on the infected device. Depending on which specific functions are being installed and used in the individual case, there may be negative effects on different levels, such as confidentiality, integrity and availability of the infected system. Moreover, owing to the intrusion potential of this technology regarding the personal life of the targeted individual, issues of freedom of expression as well as freedom of information form the core of the problem.[150] But not only is the potential for political repression relevant in this context. There is also in cases of misuse a heightened risk of social discrimination against minorities. Considering all these diverse critical issues regarding data protection and civil rights, legislative measures to regulate the use of these technologies are typically not able to keep up with the technical development in that area. However, the general use of so extensive surveillance functionalities is especially questionable in light of proportionality if just specific channels of telecommunication are to be monitored and the telecommunication service providers already installed other, less intrusive means of interception.

So for example in cases of lawful Skype call interception or chat monitoring, the principle of proportionality kicks in once the phone service is able to make the data directly available to security agencies. This may happen by a formal request to the service provider who is keeping means of wiretapping on their side of the system provision ready. In such cases, it can be assumed that a deployment of a Trojan on the target's personal device would not be needed.[151]

The monitoring of individuals also opens up issues of applicable legislation once the proxy servers involved are located outside the country borders of the deploying security agency. This was another major point criticised by the CCC in the case of the German State Trojan analysis since proxy servers were located within the United States of America.[152] Thus, the routing of potentially sensitive personal data of targeted individuals may expose it to foreign third parties performing lawful access according to the legislation of their own country. This also concerns issues of availability and integrity of the data in question.

Moreover, it seems that, in some cases, active security agencies are not aware of all possible functionalities of such complex systems, since their mostly private-company vendors are very reluctant to release the source code of their surveillance product portfolio. So it happened in cases of source code

---

[150] Cf. "›Due To Legal Issues‹ – Packet Inspection", diploma thesis of Agata Królikowski finalized for the Humboldt University of Berlin, pp. 86 ff., published March 24th 2012 and available at: http://waste.informatik.hu-berlin.de/agata/docs/due_to_legal_issues_pi_v_1_3.pdf

[151] Recent public discussions in the news have speculated about Skype providing direct access to telecommunication data processed by their servers to law enforcement agencies, see e. g. the Web Blog ijure.org article by vieuxrenard, posted January 15th 2012, "Skype likely to provide means of VoIP interception – eavesdropping by 'state trojans' disproportionate", http://ijure.org/wp/archives/833, and Craig Timberg/Ellen Nakashima in The Washington Post, "Skype makes chats and user data more available to police", news article published July 26th 2012 and available at: http://www.washingtonpost.com/business/economy/skype-makes-chats-and-user-data-more-available-to-police/2012/07/25/gJQAobI39W_story.html

[152] See CCC State Trojan report "Analyse einer Regierungs-Malware" in German, p. 3

telecommunication surveillance deployment conducted by a German law enforcement agency in the Federal State of Bavaria. According to the local Bavarian Data Protection Commissioner in charge of scrutinising the legality of the deployment from data protection view, a full review of the used surveillance system was not possible owing to missing source code. This was considered a severe violation of data protection principles the agency should have followed.[153] So it is possible that even the deploying security agencies have no full control over the technical procedures triggered once the system is brought onto the target device, nor are they able to provide verifiability to supervisory authorities without the aid of the vendor companies. This may lead to a major shortage of transparency and accountability in the context of surveillance deployment.

As for the distribution of surveillance technology to repressive non-European regimes conducted by private companies, attempts have been made to prevent such sale. For instance, the UK limited the sale of surveillance technology to Egypt, Bahrain and Libya in the wake of the Arab Spring by revoking export licences. However, the effectiveness of such sales bans remains doubtful under the consideration that export regulations may not always be applicable to the technology in question.[154] Also, democratic states may have similar interests in using such technology for analysing connection details and network communication content of individuals. Those interests may under circumstances be lawful to enhance security for the state and its citizens. But as elaborated above, a lot of questions regarding legality and proportionality arise in the context of deployment, not least because of the aforementioned inbuilt update and integration possibilities. Basically, the difference between the use of surveillance for lawful interception in democratic states on the one side and the usage of such methods to monitor citizens and potential political opponents in repressive regimes on the other side is just the configuration of the system itself.[155] For example, the same technology used in Russia to silence political opponents is also used in Germany, if only with different functionalities defined in the configuration files of the Trojan. But such a definition in configuration can be changed any time and is subject to the decision of the deploying authority.[156] So consequently, a reliable limitation of the functionalities to the boundaries of legal compliance is deemed unsure at best.

Potential Privacy by Design approaches

Under these circumstances, effective Privacy by Design approaches may be difficult to achieve. Prior to the deployment of such systems, a strict evaluation of suitability, necessity and proportionality in the narrow sense of the word should be conducted. Moreover, the deployment should be bound to a strictly pre-defined time frame as well as to a clear pre-definition of legal functionalities in the configuration. Further, limitations of functionality – as this may be guaranteed in a judge's warrant – should be put into the code of the Trojan. At best, the warrant exactly defines the allowed functionality, and the code ensures that nothing more is implemented. Also, the chosen surveillance solution should not include inbuilt update features, or the update process should be designed in a way that the updates underly the same restrictions as the Trojan itself: having undergone a strict evaluation prior to the deployment, bound to a defined time frame and to clearly defined legal functionalities. The full procedure from installation to deinstallation has to be documented in detail to ensure accountability. It has to be excluded that the Trojan can create or manipulate evidence, e. g. by putting files on the suspect's personal computer. Also it is important that the Trojan does not induce security risks by opening ports

---

153 Cf. the Bavarian Data Protection Commissioner, "Prüfbericht Quellen-TKÜ", pp. 5 f.

154 Jamie Doward in The Guardian, September 9th 2012, "Crackdown on sale of UK spyware over fears of misuse by repressive regimes" http://www.guardian.co.uk/world/2012/sep/09/block-on-exports-surveillance-equipment

155 Ben Wagner, paper for Global Voices Advocacy published 2008, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'", pp. 9 ff., available as PDF file under: http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf.

156 This is the known case for the Cisco DPI technology called "Service Control Engine" which is being used in Russia as well as in Germany, cf. Andre Meister, Netzpolitik.org blog entry November 8th 2012, "Deep Packet Inspection: Der Unterschied zwischen Internet in Diktaturen und Deutschland ist nur eine Konfigurationsdatei", available in German at: https://netzpolitik.org/2012/deep-packet-inspection-der-unterschied-zwischen-internet-in-diktaturen-und-deutschland-ist-nur-eine-konfigurationsdatei/#more-38469

in the firewall or deactivating antivirus systems. This also means that no extra devices outside the jurisdiction are used, e. g. as proxy servers collecting the user's information.

In this context, we emphasise that the increasing use of these technologies in Europe and beyond demands an intensive examination of its technical capabilities. This includes correlating an effective means of limitation to the scope of legal compliance according to the principles of a democratic system respecting human rights.

2.2.3 Smart meter surveillance

Another technology which might become increasingly relevant in the field of security is the surveillance of so-called smart meters. Especially the growing use of such devices in private homes enables a deeper insight into the everyday life of European citizens. In this chapter, we will describe the functionalities of smart meters and their capabilities to serve security purposes. Two directives[157] facilitate the implementation of smart meters in the European Union: the Directive 2006/32/EC and the Directive 2009/72/EC. The first one recommends having a close look at innovative technologies, with digital meters as one example, to give consumers the information they need to change their ways of energy consumption. The second one decrees the implementation of smart meters (80 % implemented by 2020) if an enquiry suggests that such an implementation has positive effects for the market and the individual. These examinations were done in most EU countries although not always with a focus on the individual, but more often emphasising the benefit for the market. Of course the regulation is not the first or only reason for the roll-out of smart meters.

The positive effects of a nation- or EU-wide implementation include decreased personnel costs (by remote maintenance) and shared costs for this infrastructure upgrade for the energy grid operators, better forecasting for the energy suppliers, remote deactivation of energy supplies, time-variable tariffs, monthly billing, better and promptly available information for the consumers (with the possibility of new services supplied via smart metering devices), a change in consumption habits to save money (reduced consumption estimates from 0 % to 15 % depending on the kind of feedback given to consumers[158]) and reduced CO_2 emissions throughout the EU. Another driver is the integration of renewable energy resources into the grid to further reduce CO_2 emissions. Since sun and wind are not always available for power generation, the generation profile is much more volatile compared to that of e. g. a hydroelectric power plant. So the grid has to become more flexible.

By now, the centrally generated electricity was adjusted to fit to the nation's consumption profile. In the near future there will be a lot of decentralised power generators that can't be managed in the same way (they could only be turned off if too much power is generated); therefore the consumption profile has to be adjusted to the generation (by so-called demand side management/demand response). This can only

---

[157] The Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC (revised in 2012 in the Directive 2012/27/EU of the European Parliament and of the Council of 25 October 2012 on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC) and the Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC;
References: The European Parliament and the Council of the European Union(2006): Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:114:0064:0064:EN:PDF (14.12.2012), The European Parliament and the Council of the European Union (2012): Directive 2012/27/EU on energy efficiency, amending Directives 2009/125/EC and 2010/30/EU and repealing Directives 2004/8/EC and 2006/32/EC and The European Parliament and the Council of the European Union (2009): Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC;
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:01:EN:HTML (14.12.2012)

[158] Wilma Mert, Jürgen Suschek-Berger, Johann Čas et al., "Final Report – Smart New World?" (2012)

be done in a grid which has all the necessary information and gives the respective signals to appliances – the so-called smart grid. In addition to the before-mentioned, there's also a strong technology push from companies investing in research and innovation, in product development and infrastructure for smart grids, smart homes, smart cities and so on. Smart meters have been used for a while for big electricity consumers like industrial installations. The next step is the roll-out in private households. This has been done in some countries, others are at different phases of implementation and some have decided not to implement smart meters for now. However, the aforementioned reasons have relevance for the increasing success of smart meters on the market. The biggest installation of smart meters can be found in Italy, done by Enel SpA, a company with more than 30 million customers. Some countries (e. g. the U.S. states California and Maine as well as the Netherlands) stopped the roll-out because of privacy and health concerns or at least offer a choice to consumers on whether they want to use a smart metering device or not. Others, like Sweden (finished in 2009), have a more or less nationwide roll-out.[159]

State of technology

A useful definition can be found in the final report[160] of the European Smart Metering Alliance (ESMA): Basically, smart meters are devices consisting of different units. They have a sensor metering consumed energy (for now an electrical meter, in later development and deployment states they could also integrate meters for city gas, thermal energy or water). It has a communication unit that enables two-way communication with the grid operator, a small storage device to uncouple metering and reporting intervals and a processor to handle the data. In addition, smart meters could have a display and other equipment and input devices that would facilitate the later implementation of additional services. Although one of the functions would be to give information about consumption and usage time to the customers, there exist models that don't have a display/screen built in. In these cases, it is planned to give this information via other devices like smartphones or websites. Together with the respective endpoint(s) in the operator's network, smart meters fom the advanced metering infrastructure (AMI). At the central systems the information generated and submitted by smart meters is collected and integrated into the billing system as well as different control systems, which could give information to the meters about the state of the grid, tariff information etc.

The metering units in smart meters could measure and process the electricity consumption in intervals of one second or even less. Currently it is planned to use intervals of 15 minutes. This would fit to the time slots used on the energy exchange market (where a generation surplus can be traded or energy bought in case of underproduction) where 15-minute chunks also are used. It would be possible to interlink these data to automatically get the actual energy costs which could be used as basis for the planned time-variable tariff systems.

Privacy concerns arise regarding energy usage profiling or so-called 'nonintrusive appliance load monitoring (NALM)'[161]: The usage profile of a household can be separated into the different load profiles of the respective appliances, and these load profiles can be matched against stored patterns of variable household devices. Owing to tolerances in the production of prefabricated parts most of them have slight differences even between different models of the same device and the same manufacturer, so using e. g. one Siemens microwave first and then another one, also produced by Siemens, of the same model, same output, from the same year etc., will lead to a different load pattern than using two times exactly the same microwave oven.[162] The storage of these collected metering data – even if only for a

[159] Examples can be found here: http://en.wikipedia.org/wiki/Smart_meter#Implementation_examples (17.12.2012)

[160] British Electrotechnical and Allied Manufacturers Association (BEAMA) (Ed.), "European Smart Metering Alliance – Final Report", p. 9 (2010)

[161] National Institute of Standards and Technology (NIST), The Smart Grid Interoperability Panel – Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid" (2010), p. 14; http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

[162] Klaus J. Müller, "Gewinnung von Verhaltensprofilen am intelligenten Stromzähler", article published in DuD – Datenschutz und Datensicherheit, Vol. 6/2010, http://www.secorvo.de/publikationen/verhaltensprofile-smart-meter-mueller-2010.pdf

short retention time – leads to data warehouses full of personal data.[163] Petabytes of personal data will be collected and stored every year in every European country. This collection of data may rouse the interest of security agencies in Europe for security-related surveillance purposes.

Effectiveness of smart meter surveillance and civil rights impact

Smart meters provide a number of accurate data giving insight to the energy consumption of the household they are deployed in, thus already prove very efficient in that regard. However, these metering systems show significant vulnerabilities in the security of their components and communications, exposing them to attacks. Thus we will in the following briefly describe the main weak points of these systems. Besides the fact that the current models on the market are not sufficiently protected against attacks, a major concern is the sheer number of units. There are planned to be 130 million devices in Europe in 2016[164]. In combination with the merger of electric grids and different data networks[165] this means 130 million entry points in networks that connect households with critical infrastructure. Examples in the past have shown that there is no such thing as a really secure implementation or device; there will always be a risk left. The most secure way of implementing advanced metering infrastructure would probably be a separate network with different segments and attack-safe devices (e. g. tamper-safe, moulded electronics, sealed case, data-encryption on the device as soon as the data is available etc.) in the households. With the current system, an attack on at least other households but also the grid operators is most likely going to happen within the next years. This does not necessarily mean a big blackout, but can also be an intrusion into the control network and an exchange of the only software implementing unique identifications of the smart meters, thereby ruining the complete billing system of the network operator, or blackmailing the company. Here at least financial losses are highly probable.

Reliability not only for the metering but also for the communication to and from the distribution service operator (DSO) is crucial for the advanced metering infrastructure. Examples[166] show that at least some of the devices rolled out can be manipulated quite easily to show less energy consumption. Beside the massive financial losses to the energy companies, this also brings disadvantages for other customers since some costs of DSOs are shared among all customers based on their consumption. If some of them are constantly reporting less than their actual consumption they would also pay less of the general expense. Others even cut off the smart metering device from the communication with the DSO and send fake data from their computer.[167]

A lot of different 'third parties' may be interested in the data reported by smart meters. Beside the ideas of blackmailing the DSO, launching a terrorist attack on a critical infrastructure, or stealing some energy, burglars could more easily target empty houses and flats. On the other hand there are a lot of people with access to this data. It could be either an inside job or someone spying on the communication from the smart meter. It is planned that smart meters will communicate via GSM/GPRS, Wi-Fi networks, power-line networks and/or fixed-line networks. Depending on other factors, most implementations of these communication networks are not secure for unencrypted information. Using information security

---

[163] Estimates assume an amount of 9 megabyte of data sent between each meter and the concentrator at the DSO's network per year. E. g. Austrian providers plan to roll-out about 5,000,000 smart meters, which would produce all together 42.9 terabytes of communicated data, cf. Christian Schäfer, "Effiziente Architekturen und Technologien zur Realisierung von Smart Metering im Bereich der Nahkommunikation", GRIN Verlag (2010), p. 42

[164] Heinz Arnold, "130 Mio. intelligente Stromzähler bis 2016 in Europa" (2011), http://www.energie-und-technik.de/automatisierung/news/article/80591/0/130_Mio_intelligente_Stromzxxxaumlxxxhler_bis_2016_in_Europa/

[165] What is planned can be seen in the example shown in the document of the National Institute of Standards and Technology (NIST), "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid", p. 15

[166] Brian Krebs, "FBI: Smart Meter Hacks Likely to Spread" (2012), http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

[167] Christoph H. Hochstätter, "28C3: Hacker manipulieren Daten von intelligenten Stromzählern" (2011), http://www.zdnet.de/41559104/28c3-hacker-manipulieren-daten-von-intelligenten-stromzaehlern/ (17.12.2012)

measures up to a full information security management system seems therefore advisable and should be made mandatory by the respective national or EU regulators.

A participatory technology-assessment project in Austria has shown that consumers have different requirements and requests than the industry is planning for when it comes to smart metering. [168] They are very concerned about their privacy and the security of their data, as well as the costs they will have to face when smart meters are implemented. The collected data on the consumption of electrical energy equals a comprehensive surveillance of everyday life. Energy usage profiling with 15-minute intervals would reveal how many people are living in the household, what appliances are used and when they are used[169], when they are at home and other details of their lifestyle like the preference for microwave-food or dinner cooked in three different pots with a pastry from the oven. If the interval were 2 seconds, it would even be possible to know what television programme is being watched.[170] With the help of examples like this it becomes clear how detailed the picture will be that can be derived from the data of a smart meter.

Of course such an amount of 'suddenly' available data stirs up desires of sociologists, retailers, law-enforcement agencies and credit-scoring companies. To make things worse, these data are collected at the most private area in our lives: in our homes. To protect the privacy of the home, there is a long history of laws and regulations that would protect this intimate area from the state and other individuals. The protection of the home was the nucleus for our modern understanding of privacy, which nowadays also includes the privacy of communications and personal data. An intrusion into the homes of consumers, 'spying' on them via smart meters might not be acceptable for most of them.

Potential Privacy by Design approaches

There are suggestions from different groups, like scientists, consumer protection organisations and civil rights NPOs/NGOs, on what can be done to mitigate the risks and concerns of smart metering. In many cases, the Privacy by Design approach is only possible if the entire system is being changed, or essentially redeveloped.[171] This shows the deficiencies of many of today's smart meter implementations that have not been designed taking sufficiently into account privacy requirements. The measures described in the following rather try to mitigate some problems of the current concepts instead of proposing a new design.

- ***Technical measures***

Authentication between meters and network

In planned implementations, every smart meter gets a certain software ID. But there is no authentication between the smart meter device and the network that would help to identify unauthorised devices in certain network domain environments. Here authentication methods should be integrated to prevent or at least identify unauthorised components.

---

168 Mert/Suschek-Berger/Čas et al., "Final Report – Smart New World?" (2012)

169 National Institute of Standards and Technology (NIST), "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid" (2010), p. 13

170 Ulrich Greveler, Benjamin Justus, Dennis Löhr: "Identifikation von Videoinhalten über granulare Stromverbrauchsdaten", Proceedings of Sicherheit 2012, LNI P-195, pp. 35-45 (2012);
Ulrich Greveler, Benjamin Justus, Dennis Löhr: "Forensic content detection through power consumption", ICC 2012, pp. 6759-6763 (2012).

171 Alfredo Rial, George Danezis, "Privacy-Preserving Smart Metering", Proceedings of WPES 2011, pp. 49-60 (2011);
Klaus Kursawe, George Danezis, Markulf Kohlweiss, "Privacy-Friendly Aggregation for the Smart-Grid", Proceedings of PETS 2011, pp. 175-191 (2011);
Marek Jawurek, Florian Kerschbaum, George Danezis, "Privacy Technologies for Smart Grids – A Survey of Options". Microsoft Technical Report MSR-TR-2012-119, November 2012, https://research.microsoft.com/apps/pubs/?id=178055;
Félix Gómez Mármol et al., "Privacy Enhanced Architecture for Smart Metering", International Journal of Information Security, vol. 12 no. 2, pp. 67-82 (2013).

Encryption

Data has to be encrypted end-to-end from the time it is collected by the metering unit in the smart meter, across processing, storing and transmission, up to backup and archiving solutions until deletion.

Segmentation of networks

As shown above, it might be wise to segment different networks instead of merging them, maybe even segmenting a network itself. If a security incident occurs, it will be easier to keep the network up and running if intruders can only access small parts of it.

Hardening devices

As mentioned above, the devices could be built in a way that makes manipulation more difficult. As a starting point, the construction of a POS card terminal or a pin pad equipped smart card reader could be used as a model, since most of them can't be opened in a non-destructive way. Some of them even feature sensors detecting any tampering attempt, which leads to a reported incident and a system shutdown.

Expiration dates for personal data

Personal data have to be deleted as soon as possible. A way of technically ensuring limited access to the collected data would be encrypting it with an expiration date after which the keys to decrypt them are not valid anymore.

➢ *Organisational measures*

Designing privacy measures in the implementation/roll-out could also mean using organisational measures to complement the technical measures, and as soon as organisational measures are agreed upon, technical measures can support them. For billing purposes, it would be sufficient to collect data on the consumption once a month. For forecasting and demand response, 15-minute intervals may be necessary, but this data can be completely anonymised and needs not to be as detailed or on a household basis. So a solution for the privacy dilemma might be to separate the data. The grid operator gets the anonymous data every 15 minutes summed up from at least 250 households. The energy supplier gets the sum once a month for each household and has to delete the data after the period of objection against the billing.[172] The consumer gets the actual and aggregated consumption data directly from the metering device without a loop via other systems and can decide on how long it should be stored (encrypted) on the device. Feedback data from the grid operator to the smart meter devices could be sent via broadcasts to the respective network segments. Of course this requires tamper-safe metering devices which are smart enough to process only authorised programs, so any attempt to attack the metering device can either be fended off or at least detected with the consequence of stopping the processing. Another idea to mitigate the risks of surveillance would be to decrypt the meter's data only with the consent of the possessor (given by his/her own key, together with the ones from the DSO).

As mentioned above, a complex environment like a smart grid with smart meters in every household is a system with a lot of entry points and potential security risks. To manage situations like this there exist different best practices and international standards (like the ISO/IEC 27000 family of standards) which should be applied and certified for the whole network, end-to-end from the household metering devices to the central data processing and storage[173]. In addition, also privacy certificates (like the European Privacy Seal EuroPriSe[174]) should be earned. As already stated, additional organisational measures can lay the foundation for supporting technical measures. Examples of such measures are unified standards for data access and making the data processes transparent for the concerned citizens.

---

[172] Compare to: Klaus J. Müller, "Gewinnung von Verhaltensprofilen am intelligenten Stromzähler", DuD issue 6/2010

[173] See also the Article 29 Working Party: "Opinion 12/2011 on smart metering" (WP 183), p. 19., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf (14.12.2012)

[174] http://www.european-privacy-seal.eu/ (15.12.2012)

In recent years, different stakeholders have pushed for a widespread adoption of smart grid and smart meter implementation throughout Europe. This is due to the need for improved energy consumption forecasting and enabling optimised processes of energy supply at low costs. However, the establishment of smart meters enables these companies to obtain significant insight regarding the lifestyle and behaviour of European citizens. In this context, the Article 29 Working Party addresses the legitimacy of data processing for crime detection or prevention, stating that *'the detailed picture obtained by smart meters that inform suppliers about patterns of energy use might allow for the identification of suspicious and, in some cases, illegal activities. The Working Party would remind the industry that the fact that such a possibility exists does not automatically legitimise wide-scale processing of data for this purpose.'* [175] It is yet to be seen if appropriate standards in this field of technology can be developed which are more suitable to creating a balance between safety measures and supply security on the one side and the privacy of European citizens on the other.

2.2.4 Location tracking

The modern days of mobile communication have led to a significant expansion of technologies providing a variety of location systems. These serve a multitude of different purposes in several areas, ranging from military, health care, retail and postal. The mobility of persons and assets has thus become another aspect of security in public space, thus reinforcing the desire of intelligence and police agencies to obtain geo location information where needed. In an attempt to define the difference between location and geo location, it can be said that location is a more vague term relating to a certain attribute, such as a city district or street name; geo location, however, is represented by very precise geographic position information by means of latitude, longitude and altitude coordinates.[176] In this context, most real-time location systems nowadays are built-in wireless systems. Most of these technologies entail a so-called location-based system which consists of five basic components needed for the functionality of the service. [177] These components are:

- Software application of the service provider
- A mobile network to transmit data and requests for the service
- Content provider supplying the geo-specific information
- A positioning component (GPS)
- End-user's mobile device

Thereby, the mobile devices equipped with such a location-based service make the monitoring and tracking of their users possible. Within a security context, these capabilities enable the concerned authorities to locate, track and possibly identify persons and assets which potentially pose a threat to public security. For this document, we focus on some core technologies enabling such events, which are specifically GPS, cell tower records and Silent SMS. These are in the following called 'location trackers' and will be described in the subsequent sections.

GPS

Global Positioning Systems (GPS) were originally developed for navigation purposes and have become in recent years broadly deployed as a commonplace technology on a multitude of devices. The technology works generally by transmitting timing data with atomic-clock precision to the receivers they are linked to. Thus, several application fields determine the main deployment areas of GPS systems. These are:

---

[175] Article 29 Working Party (WP 183), p. 21

[176] Cf. Margaret Rouse on SearchmobileComputing, definition entry for the term "Geolocation", http://searchmobilecomputing.techtarget.com/definition/geolocation

[177] Cf. Margaret Rouse on SearchNetworking, definition entry for the term "Location-based service (LBS)", searchnetworking.techtarget.com/definition/location-based-service-LBS

- Positioning
- Navigation
- Precise timing (e. g. by power grids to create & use time stamps for power-line fault monitoring)
- Frequency calibration (e. g. for cell phone towers together with the precise timing function)

In order to calculate the precise 3D space location and time, the GPS receivers perform a trilateration. This means that the distance from four or more GPS satellites is measured, whereby each satellite represents a dimension in space-time (see Figure 6).

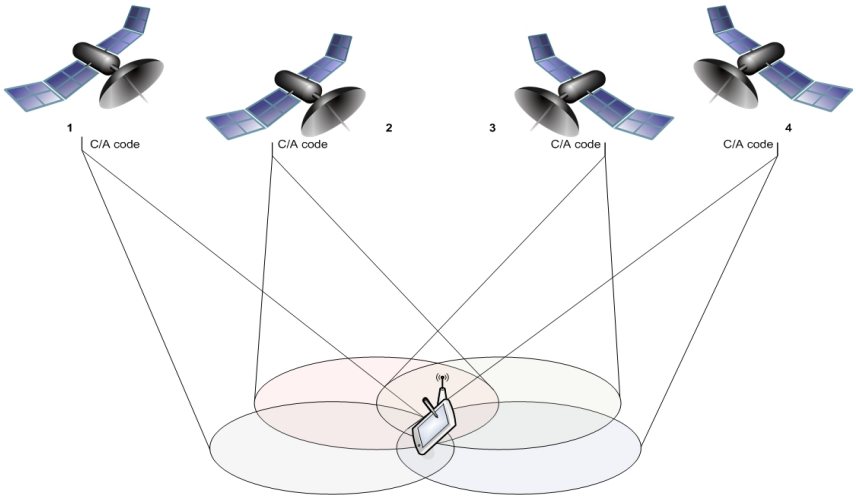

Figure 6: GPS receiving satellite signals to determine exact time and geolocation

Each of these GPS satellites streams a coarse acquisition (C/A) code at a 1 ms interval. In the field of civil usage, such code stream is usually unencrypted and does not require authentication.[178] The C/A code is basically a unique, public pseudo-random number (PRN) which is generated by the satellite. On top of the satellite's C/A code, a navigation message is attached with data usable for navigation. So for instance, this data includes the current time from the atomic clock of the satellite, the week number, and other information relevant for navigation. When the GPS receivers get the data from this stream, this means they have obtained a replica of this code. The receivers then assess the time required to align the original code of the satellite and the local replica code, a procedure also called time delta estimation. This time delta estimation allows the receiver to precisely determine the distance to that single satellite. This distance measurement is also called pseudorange. Beyond the distance information, more data are assessed to determine the exact position and the clock offset of the satellite. From all this information,

[178] This is different for the usage of GPS in the fields of governmental or military deployment, or for critical infrastructures. Further research to enhance effectiveness and security in these fields is currently on-going. For example, the European Commission fosters the research within the Galileo programme, which offers a secure encrypted global navigation satellite system, see the navipedia website entry of the European Space Agency (esa) about the Galileo Public Regulated Service (PRS) with links to further informational sites: http://www.navipedia.net/index.php/Galileo_Public_Regulated_Service_%28PRS%29; in Russia, a similar programme for civil use named GLONASS exists, which is also expected to become significant for commercial uses, cf. Lorenz Hilty, Britta Oertel, Michaela Wölk, Kurt Pärli, Zentrum für Technologiefolgen-Abschätzung (TA-Swiss, translated: Centre for Technology Assessment), "Lokalisiert und identifiziert – wie Ortungstechnologien unser Leben verändern" (translated: "Located and identified – how localization technologies change our lives") (2012), p. 18, http://www.ta-swiss.ch/ortungstechnologien/

the receiver is then able to calculate a 3D space and time frame.[179] Depending on the receiver in use and other factors, such calculations are potentially so precise that is possible to determine the position of a device with an integrated GPS receiver accurately within a millimetre range.[180] Further developments in the field of GPS technology include the distribution of so-called GPS dots. These are small, no more than button-sized, GPS tracking devices providing data accurate enough to locate an individual or item with high precision.[181]

The positioning and timing functions of GPS are relatively vulnerable to manipulations and attacks. Two of the most prominent examples are GPS jammers and GPS spoofing: GPS jammers basically disrupt the data stream from the satellite by transmitting noise into the frequency band, so the receiver is no longer able to connect with the satellite. However, GPS jammers pose a quite significant security threat because they affect not only the receiver they are intended for. Rather, they function like a thick signal blanket for all receivers within their range, which can extend for miles. And it is possible that some of these receivers might be crucial for dependent critical infrastructure systems, like devices in hospitals, lighthouses, power grids, ships, public transport and so on. Owing to this reason, GPS jammers are illegal in many countries. A GPS spoofing attack, however, is set up directly onto the receiver, feeding it with bogus input data to achieve faulty pseudorange calculations.[182] This is done by using a device creating false civil GPS signals, tricking the receiver into a miscalculation of 3D location and timing. A recent demonstration of the effectiveness of such a spoofing attack was given by Cockrell School researchers from the University of Texas, who succeeded in misleading a GPS-dependent drone using a spoofing attack. A possible countermeasure could be, as it is already commonplace in the military field, the encryption of data signals in the civil usage areas of GPS.[183]

In fact, there is a multitude of different conceivable attacks on GPS, ranging from software to hardware sabotage and manipulation, e. g., data level attacks, receiver software attacks or attacks of the dependent system. Possible scenarios are the manipulation of positioning, navigation and timing data of planes, cars, trucks, ships and personal devices of individuals. Moreover, the manipulation of reference stations can be used to amplify attacks. In this context, a reference station is a network providing information to dependent individual receivers. Examples of such networks are the FAA Wide Area Augmentation System (WAAS) being used for airplane flight, the CORS network and the NTRIP receivers for surveying and unmanned vehicle navigation. Another attack field could be the down-stream feeding the computer system the receiver is part of, where the RF port and the Ethernet port of the devices have proven especially vulnerable. The broad range of these aforementioned attack methods and areas show that while a correctly functioning GPS system provides extremely accurate location and timing data, further research on the possibilities of and potential countermeasures against GPS vulnerabilities is critical for the stability and reliability of this already widely deployed technology.[184]

---

179 Tyler Nighswander, Robert Brumley, Brent Ledvina, David Brumley, Jonathan Diamond in "GPS Software Attacks", p. 1, CCS'12 paper published in October 2012, available at: http://users.ece.cmu.edu/~dbrumley/courses/18487-f12/readings/Nov28_GPS.pdf
For a more in-depth elaboration, see Jörg Roth, University of Hagen, in "Location-Based Services" by Jochen Schiller & Agnés Voisard, Chapter 7 "Data Collection" encompassing an explanation of basic location techniques, triangulation/trilateration/traversing and satellite positioning systems.

180 Cf. J. B. Barnes and P. A. Cross, Department of Geomatic Engineering of the University College London, research paper conducted for the Department of Geomatics, Newcastle University and supported by the EPSRC and Trimble Navigation, published in 1998, "Processing models for very high accuracy GPS positioning", p. 1, http://www.gmat.unsw.edu.au/snap/publications/barnes_etal98a.pdf

181 Todd Humphreys, The Cockrell School of Engineering/The University of Texas at Austin, TEDx video and script, March 8th 2012, "The GPS Dot and Its Discontents", http://www.engr.utexas.edu/features/7233-humphreysgps

182 Cf. Nighswander, Brumley, Ledvina, Brumley, Diamond, "GPS Software Attacks", p. 1

183 Cockrell School of Engineering of The University of Texas at Austin, "Cockrell School Researchers Demonstrate First Successful 'Spoofing' of UAVs"; and Todd Humphreys, "How to fool a GPS"

184 See Nighswander, Brumley, Ledvina, Brumley, Diamond, "GPS Software Attacks", pp. 2 ff., where the novel attack scenarios and the possible application fields are described in more detail.

Cell tower records for mobile phone location data

In order to track a mobile phone, the current position of the device must be obtained. As explained above, this can already be conducted very accurately in cases where the device has an inbuilt activated GPS positioning system. However, there are alternative methods of determining the location of the device. To ensure that the correct mobile device was targeted with the localisation effort, certain identifiers are needed. Such identifiers can be:

- Subscriber Identification Module (SIM)
  - A removable smartcard
- International Mobile Equipment Identity (IMEI)
  - A unique 15-digit serial number of the device
- International Mobile Subscriber Identity (IMSI)
  - A 15-digit number containing country & network code & identification number parts[185]

One method of locating a mobile without GPS would be the so-called cell tower record. In order to provide their services, telecommunication providers rely on radio signals to determine the current location of the mobile phone, respectively its owner or possessors. A mobile phone always maintains a connection to the nearest antennas and base stations. This is typically done by these radio signals which are sent back and forth between one or several radio or cell towers of the network provider which is integrated into its infrastructure and the phone itself. Through the radio signal connection the distance between a cell tower and the phone can be estimated. So basically, the cell tower location itself and its range indicate at least the rough location of the device. The range of the tower, i. e. the size of the cell, however, is determined by the geographic features of the area and the number of possible calls which must be handled simultaneously. Usually, in more populated areas, the cell may be quite small (like a few hundred meters), whereas in more rural areas it may be significantly larger (several kilometres).[186] Once the mobile phone changes its location and moves throughout several cells, the connection to the cell tower is always handed over to the next tower which transmits the strongest signal within the reach of the device (also called 'handover' or 'handoff').

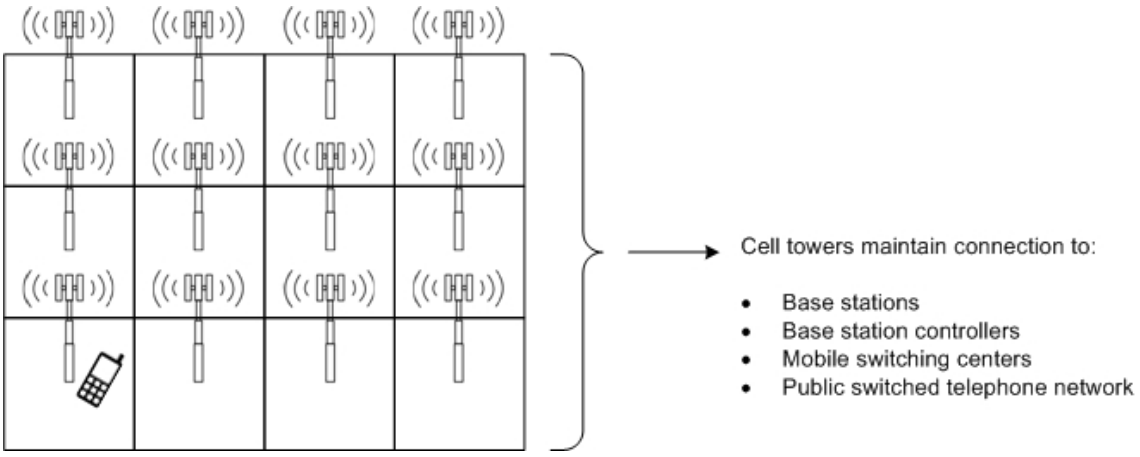

Figure 7: Radio signal tower cells of a GSM network indicating the location of a mobile phone (simplified model)

The radius of the cell tower itself allows for only rough location estimation within the diameter of the cell. As mentioned, this diameter can vary greatly, which makes accurate localisation, especially in rural

[185] Cf. the introductory descriptions by Daehyun Strobel, Ruhr-University Bochum, Chair for Communication Security, in the publication "IMSI Catcher" from July 13th 2007, pp. 4 ff.
[186] Ibidem, p. 4

areas, difficult. However, the towers closest to the mobile phone can be used in a triangulation calculation to further narrow down the location. Triangulation means that the distance to the towers closest is measured together with the speed of the signal to calculate more precise position, taking into account the delay until signal arrival.[187] Within the infrastructure of the telecommunication provider, the cell towers maintain constant connection to base stations and base station controllers (see Figure 7). These in turn are connected to mobile switching centres which again are tied to the public switched telephone network. In this context, the mobile switching centre is tasked with the mobility management and thus has access to four different data bases necessary. These data bases are and contain:

- Home Location Register (HLR)
  - Personal information of the subscriber, e. g. IMSI, the phone number or the GSM services
- Visitor Location Register (VLR)
  - Dynamic information of the subscribers, which are mostly copies of the HLR data
- Authentication Centre (AuC)
  - Access data of every subscriber
- Equipment Identity Register (EIR)
  - Data base of IMEI numbers of banned stolen phones to prevent those from accessing the network[188]

The European Telecommunication Standards Institute (ETSI) developed the open standard GSM (Global System for Mobile Communications) that describes protocols for most digitally switched networks used by mobile phones. It fits to so-called second generation (2G) digital cellular networks designed for mobile telecommunication devices. Succeeding GSM, the Universal Mobile Telecommunications System (UMTS) was developed as a standard of the third generation (3G) networks. The UMTS was developed as a standard with higher data transmission performance and improved security features, for example providing mutual entity authentication between mobile phone and the Mobile Switching Centre (MSC)/HLR (also called home environment). Owing to the aforementioned nature of the mobile network functionality, security agencies wanting to surveil e. g. a specific area have the ability to turn to the network provider in order to obtain the information from the cell tower data bases. In case the security agencies are interested in the location of a specific device and its owner, they will need specific identifiers to match them with the information from these data bases. Either way, with a so-called cell tower dump, security agencies can for a specific area and time frame obtain information about incoming and outgoing calls, SMS and position of the devices in the area.

The localisation of a mobile phone by its connection to the closest cell tower is only possible if the phone is technically connected with a cell tower. This is usually the case if a phone is switched on (and not in 'flight mode') and the network is available. If the phone itself or its data connection is turned off, the link to the next cell tower is not existent, and thus derives no information regarding the whereabouts of the device. It may be possible to prepare a cell phone with spyware so that it will pretend to be turned off, but this requires direct access to the device itself.

Silent SMS

Another possibility to locate a mobile phone (and to receive the IMSI code of the device for further usage) is the Silent SMS, also called Stealth Ping. This method has originally been developed to enable network operators to determine if a phone is switched on and to test the network performance without the knowledge of its users. Short Message Services (SMS) are basically communications between individual mobile devices enabled by the mobile network. This network allows single peer-to-peer

[187] This is slightly different to GPS positioning, where trilateration is used, triangulation simply connects two fixed positions from where the angle to the location is measured (think of two intersecting lines). In a trilateration calculation (for GPS), two fixed positions are also used, but added up to two distances to the unknown location (think two intersecting circles). In contrast to triangulation, trilateration leads to nonlinear equation not entirely suitable for 3D positioning, thus requiring additional numeric methods during the calculation.

[188] Daehyun Strobel, "IMSI Catcher", pp. 5 f.

messages, but also mass-application generated SMS being passed through the Mobile Switching Centre while using certain message protocols. The Silent SMS process goes as follows: It is necessary to know the mobile phone number of the person to be localised. To send the Silent SMS, a SMS gateway of the provider's network is used to distribute a message without real content and with altered data coding scheme values, which causes the receiving device to remain quiet. The device itself will give no signal and registers no incoming message arrival.[189] Thus, the Silent SMS will leave no trace. But it triggers a backping to the network provider, which contains the internal IMSI code derived from the SIM of the mobile phone. With the help of this code, the owner of the mobile phone can be identified and the location determined by the cell the signal came from.[190]

It is also possible to use a greater number of Silent SMS to be sent towards the same destination, e. g. for tracking a person over a period of time. Since it is technically easy to send a high number of messages within an hour at low costs, this method is also to suitable for emptying the batteries of the mobile device in short time.[191] In this context, it should be mentioned that the Silent SMS only work in cases where the battery has not been removed from the device.[192] After the message has been sent, security agencies can contact the network provider for a cell tower dump or instead for an already prepared real-time map showing the movement profile of the mobile device.

Effectiveness of location trackers and civil rights impact

In recent years, it became known in several countries that the mass application of location trackers has become fairly pervasive.[193] All these above-mentioned and described methods of location tracking have one thing in common: the location data are collected and processed in order to technically provide the network services of a mobile device. These services may range from the standard functionality of mobile phones to route incoming or outgoing calls, to accurate geolocating, navigation and timing. The data being collected and processed during these tasks are needed by the network providers to ensure the functionality of the requested services. But especially repeatedly collected or requested location data, even in anonymised or pseudonymised form, may reveal information about frequently visited places, enable predictions about future whereabouts, determination of means of transportation (by foot, car etc., how fast the person is moving), allow an assessment of likely living or work places, and last but not

---

189 Fabien Soyez, QWNI News website article of January 27th 2012, "Getting the Message? Police Track Phones with Silent SMS", http://owni.eu/2012/01/27/silent-sms-germany-france-surveillance-deveryware/; see also an overview of the most common values of data coding schemes on the website of the company CardBoardFish at http://www.cardboardfish.com/support/bin/view/Main/DataCoding

190 Cf. European Digital Rights (EDRI), website entry of February 1st 2012, "Police frequently uses Silent SMS to locate suspects", http://www.edri.org/edrigram/number10.2/silent-sms-tracking-suspects

191 Cf. Neil J. Croft, Martin S. Olivier, "A Silent SMS Denial of Service (DoS) Attack", Southern African Telecommunication Networks and Applications Conference 2007 (SATNAC 2007) Proceedings, published 2007 and online as PDF file available under: http://mo.co.za/abstract/silentdos.htm; In recent years, it was revealed in several countries that this mass application of Silent SMS has become fairly common. For examples, see F-Secure Blog entry of December 29th 2011, "440,783 'Silent SMS' Used to Track German Suspects in 2010", https://www.f-secure.com/weblog/archives/00002294.html, and Eric Lichtblau in The New York Times, "Wireless Firms Are Flooded by Requests to Aid Surveillance", July 8th 2012, http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?_r=2&ref=surveillanceofcitizensbygovernment

192 Peter Maass, Megha Rajagopalan, New York Times Sunday Review article of July 13th 2012, "That's Not My Phone. That's My Tracker", https://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html?_r=3&src=rechp

193 For examples, see: F-Secure Blog entry of December 29th 2011, "440,783 'Silent SMS' Used to Track German Suspects in 2010", https://www.f-secure.com/weblog/archives/00002294.html; Eric Lichtblau in *The New York Times*, "Wireless Firms Are Flooded by Requests to Aid Surveillance", July 8th 2012, http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?_r=2&ref=surveillanceofcitizensbygovernment; Kevin Bankston, article of December 1st 2009 for the Electronic Frontier Foundation, "Surveillance Shocker: Sprint Received 8 MILLION Law Enforcement Requests for GPS Location Data in the Past Year", https://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law

least make the identification of the individual possible.[194] This is also being discussed in the context of the European Data Retention Directive 2006/24/EC that requires telecommunication and Internet providers to store and retain traffic data of all users for at least six months for the sole purpose of law enforcement.[195] But at least the method of mass data requests currently proves difficult for real-time surveillance. However, cell tower data or data retained on the basis of the Data Retention Directive are increasingly being requested. Critics point out that since a strict targeting, i. e. a specific reduction of requests to data of certain individuals, is not possible, this broad measure mostly concerns data of innocent citizens being put under general suspicion.[196]

The positioning, location and tracking of mobile devices may be prevented or circumvented by using different techniques. But these come with significant disadvantages and dangers, as we described above in the context of GPS jamming and GPS spoofing.[197] Thus the difficult question is how to ensure the privacy of the network user when this data is necessary to subscribe to the offered services. The very nature of these services requires a timely positioning/location of the mobile device the individual is using. Thus, the whole system is prone to the creation of location and movement profiles of individuals, possibly even in real-time. This proves especially problematic for those technologies where it is not possible to predetermine whose data shall be collected. Then, a mass collection of personal data is conducted, which will in most cases affect primarily innocent citizens without tangible evidence of crimes. Consequently, the application of these location tracking techniques inherently implies a general suspicion of everyone present in the area being surveilled, raising significant issues regarding the proportionality of the measure. Also, this leads to a large potential of chilling effects regarding freedom of expression and freedom of association, e. g. at political demonstrations. Moreover, sensitive data might be obtained, e. g. by the revelation of the individual being present in the offices of medical professionals, psychologists, lawyers etc.

Other habits of the individual may also be revealed simply by geo location profiling. So for example, in a case ruled on by the United States Court of Appeals for the District of Columbia Circuit which was related to the tracking of an individual by means of GPS, it was stated that by a steady geo tracking, it can be found out if the person *'is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.'*[198] Moreover, a study about predictive modelling suggests that a cross-referencing of the obtained data with the data of the social environment of the targeted individual enables quite accurate predictions of potential future whereabouts.[199] Also to be considered must be for how long the respective telecommunication providers will retain the gathered data in its data bases.

---

194 Hilty/Oertel/Wölk/Pärli, "Lokalisiert und identifiziert – wie Ortungstechnologien unser Leben verändern", p. 71

195 Data Retention Directive: "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC"

196 Cf. Trevor Timm, Electronic Frontier Foundation (EFF), "Law Enforcement Agencies Demanded Cell Phone User Info Far More Than 1.3 Million Times Last Year", July 9th 2012, https://www.eff.org/deeplinks/2012/07/law-enforcement-agencies-demanded-cell-phone-user-info-much-more-13-million-times;
another example is the public discussion in Germany regarding mass cell tower requests in the context ot the NSU investigations, cf. Andre Meister in Netzpolitik.org, "Funkzellenabfragen bei NSU-Ermittlungen: 20 Millionen Verbindungsdaten, 14.000 Namen und Adressen, 0 Täter", October 19th 2012, https://netzpolitik.org/2012/funkzellenabfragen-bei-nsu-ermittlungen-12-millionen-verbindungsdaten-14-000-namen-und-adressen-0-verdachtige/

197 Cf. Nighswander, Brumley, Ledvina, Brumley, Diamond, "GPS Software Attacks"; Todd Humphreys, "The GPS Dot and Its Discontents"

198 Citation from the ruling No. 08-3030 of the United States Court of Appeals for the District of Columbia Circuit issued August 6th 2010

199 David Talbot, "A Phone that Knows Where You're Going – An algorithm can better predict your future movements by getting a little help from your friends", MIT Technology Review, July 9th 2012, http://www.technologyreview.com/news/428441/a-phone-that-knows-where-youre-going/

Potential Privacy by Design approaches

Owing to the above-described nature of the communication, navigation and timing services being offered by the respective network providers, the collection and processing of personal data seems unavoidable in the currently established architecture. However, since more than fifteen years data-minimising architectures have been proposed in the scientific community.[200] Also, ideas to limit law enforcement requests to the scope that is needed for a specific situation instead of retaining personal data of all citizens have been discussed.[201] However, potential Privacy by Design approaches from the technological side are yet to be developed. In this context, possible research areas look promising in the field of anonymous authentication towards the network, pseudonymisation of network identifiers, new techniques of pinpoint location dissipation or obfuscation, and improved encryption of communications.[202] Until such research has achieved a sufficient level of efficiency and deployment, any privacy-preserving approaches in this field will for the time being mostly entail organisational measures to restrict access to the data bases. At least, it is possible to strive for improved IT security of the systems themselves to counter weaknesses of the respective technologies and their settings (e. g. in the GSM networks) as well as to prevent unauthorised access by unauthorised third parties.[203]

2.3 Biometrics & body scanners

Biometric recognition systems and body scanners are two fields of technology being closely tied to the bodily integrity of the concerned target individual. The international Association for Identification defined biometrics as referring *'to the measurement and analysis of attributes of living things'*.[204] The International Organization for Standardization (ISO) developed a series of biometric data format standards known as ISO/IEC IS 19794. The ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV)[205] understands biometrics as *'biological and behavioural characteristics of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition'*. Thereby, biometric recognition encompasses both biometric verification as well as biometric identification. However, the goal of most biometric recognition systems is either the identification of an individual, or the verification/falsification of a claimed identity. Though not a conclusive list, examples of such measurable biological and behavioural characteristics are:

- Face topography & facial expression

---

200 Hannes Federrath, "Vertrauenswürdiges Mobilitätsmanagement in Telekommunikationsnetzen" (translated: "Trustworthy mobility management in telecommunication networks"), Dissertation, Technical University of Dresden, Informatics Faculty, February 1998

201 Stefan Köpsell, Rolf Wendolsky, Hannes Federrath, "Revocable Anonymity", Proceedings of ETRICS 2006, LNCS 3995, pp. 206-220 (2006);
Marit Hansen, "Concepts of Privacy-Enhancing Identity Management for Privacy-Enhancing Security Technologies", D 7.3 PRISE Conference Proceedings: "Towards privacy enhancing security technologies – the next steps" (2009), pp. 91-103, http://www.prise.oeaw.ac.at/docs/PRISE_D7.3_Concluding_Conference_Proceedings.pdf;
Stefan Köpsell, "Entwicklung und Betrieb eines Anonymisierungsdienstes" (translated: "Development and operation of an anonymising service"), Dissertation, Technical University of Dresden, Informatics Faculty, March 2010

202 Cf. Julien Freudiger, École Polytechnique Féderale de Lausanne, "When Whereabouts is No Longer Thereabouts: Location Privacy in Wireless Networks", pp. 29 ff., published 2011 and available at: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDMQFjAA&url=http%3A%2F%2Finfoscience.epfl.ch%2Frecord%2F154767%2Ffiles%2FEPFL_TH4928.pdf&ei=bSLwUKeZIcOstAbe84DICw&usg=AFQjCNGmDTe7IVfVENCrPG9lx3S83xGGmA&bvm=bv.1357700187,d.Yms&cad=rja

203 In July 2012, the German security expert Collin Mulliner pointed out the high risks of inadequate IT security in mobile devices by proving the data obtainment from mobile networks by means of a simple port scanner, see Heise Security blog entry of July 27th 2012, "Scan in Mobilfunknetzen fördert tausende ungeschützte Geräte zu Tage", available in German at: http://www.heise.de/newsticker/meldung/Scan-in-Mobilfunknetzen-foerdert-tausende-ungeschuetzte-Geraete-zu-Tage-1653619.html

204 International Association for Identification (IAI), website information under "Biometrics Information Systems" http://www.theiai.org/disciplines/biometrics/index.php

205 As defined in the SC37 Working Group 1 for the International Biometrics Standard ISO/IEC 2382-37.

- Skin texture & colour
- Hand & finger topography
- Ridge structure of hand palm
- Iris structure & retinal pattern
- Vein structures
- DNA
- Signature pattern & dynamics
- Voice acoustic patterns

All of such or similar information obtained by biometric measurement methods may under circumstances be subjected to access by security agencies for purposes of crime prevention and crime investigation. This is also due to the fact that biometric characteristics are typically bound to an individual, whereas other identification or authentication systems, such as code, secret password, or the possession of another physical identifier, may be just temporary. Regarding these characteristics, a distinction must be made between so-called static and dynamic characteristics. Static characteristics do not or sparsely change over the lifetime of the individual, such as fingerprints, genetic information etc. Dynamic characteristics are behavioural traits of an individual, such as written signature, facial expression, movement and voice patterns etc.[206]

Biometric and body scanner technologies have in the past years been increasingly deployed in various fields relevant in the context of security. So, for example, biometric systems were already used in 1996 to perform checks on 65,000 athletes and staff during the Atlanta Olympics.[207] So there is a multitude of opportunities to perform biometric recognition, which would require a complete in-depth analysis of their own. Thus, we will in this document focus on one of today's very relevant biometric measurements, namely systems for facial recognition. Moreover, information obtained by body scanner technology is also often subjected to data collecting activities of governmental security bodies. At first glance, body scanners seem to be a technology not directly related to biometrics at all. But while body scanners are not by definition biometric recognition systems, they may also lead to the collection, processing, and storage of biometric data. They are currently used at several airports across Europe and beyond to enhance the security of international airport transportation. So we will in the following also describe full body scanner technology to provide for an overview of the main functionalities of this technology.

2.3.1 Facial recognition

Humans predominantly use face recognition to verify the identity of an individual or to perform an identification process. Facial recognition is also one of the biometric techniques being used for this purpose. Since the face of a person is usually visible (unless the person wears a veil, a hood, a helmet or a mask), this biometric method works without cooperation of the person concerned, e. g. when analysing a photo or a video, no matter whether the visual image is taken from a CCTV system or a social network. Already deployed in a number of European and other countries for the enrolment of electronic IDs, it can be used to enable physical or virtual access restriction.[208] Scientists and developers envision

---

[206] Cf. the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), "Einführung in die technischen Grundlagen der biometrischen Authentisierung" (translated: "Introduction into the basics of biometric authentication"), p. 1, available in German at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf?__blob=publicationFile

[207] Michelle C. Frye, Master of Arts thesis submitted to the Faculty of the Graduate School of Arts and Sciences of Georgetown University, "The body as a password: Considerations, uses, and concerns of biometric technologies", p. 46, April 27th 2001, including further examples throughout the history of biometrics development.

[208] Cf. Rebecca Bowe for Electronic Frontier Foundation, "2012 in Review: Biometric ID Systems Grew Internationally … And So Did Concerns About Privacy", December 29th 2012, giving a brief overview of current developments in the European Union, Mexico and India. Also see the Federal Commissioner for Data Protection and Freedom of Information in Germany, "Biometrics and chip identity cards in every day working life", www.bfdi.bund.de/EN/Topics/labour/Artikel/BiometricsChipIdentities.html

further applications for facial recognition, e. g. in e-commerce in combination with the use of Smart Cards e. g. for online banking[209], and in covert surveillance conducted by governmental security agencies.[210] Within potential civil use, facial recognition as part of a wider spectrum of biometrics is interesting to companies owing to a number of reasons. So key explanations of its widespread adoption not only include its prevention of unauthorised access and fraud, but also its enhancement of administrative efficiency. Entities that use facial recognition systems may see potential benefits in a great variety of areas, for example:

- Administration costs
- Identification & information integrity
- Physical and virtual access control
- Delivery speed regarding services and benefits
- Research and statistics accuracy and quality
- Targeted advertising, e. g. within social networks
- Technical security of communication[211]

Some of these aspects also play a role in governmental uses of biometrics. Deployed mostly covertly as a surveillance tool at airports, public buildings, banks or larger public spaces often used for events, facial recognition seems accepted by citizens as means of enhancing public and state security in these areas. Moreover, facial recognition may also be used in investigation cases for forensic purposes. The simplest use of facial recognition is the conventional face detection process. More sophisticated uses of this technology allow for an assessment of the facial characteristics regarding, e. g. age, gender, race, mood or emotion.[212] So it is little surprising that facial recognition technology is more and more commonly deployed in a variety of areas to fight crime by detecting and identifying suspects. In the U.S., the Federal Bureau of Investigation (FBI) just obtained a $1 billion budget to further continue the so-called Next Generation Identification (NGI) project, which aims at rolling out a unified biometrics system to be deployed across the whole nation by 2014.[213] Research in this field is also being conducted in Europe. However, the ethical, civil rights and privacy-related issues linked to biometric technologies have been long neglected despite their widespread use. Even in 2011, the Council of Europe issued a statement that it would not investigate the legality of the current national biometric schemes in light of Article 52 of the European Convention on Human Rights.[214] But these problematic issues of biometric technologies in general increasingly become the focus of on-going European Commission funded research projects within Europe. Some examples of such projects, not necessarily working with facial recognition, are:

---

[209] Cf. a study conducted by Thomas F. Dapp and commissioned by the Deutsche Bank, "Growing need for security in online banking", published February 8th 2012

[210] Cf. Walter Kropatsch, Robert Sablatnig, Pattern Recognition and Image Processing Group at the Institute of Computer-aided Automation, Computer Science Department of the Vienna University of Technology, "Biometrics", p. 5

[211] Cf. Simon G. Davies, Department of Law, University Of Essex, "Assessing Biometrics and Privacy and Touching Big Brother – How biometric technology will fuse flesh and machine", published in Information Technology & People, V 7, N. 4 1994, https://www.privacyinternational.org/reports/assessing-biometrics-and-privacy-and-touching-big-brother; moreover, regarding the usage for targeted advertising, see Konrad Lischka for Spiegel Online, "Marktforschung per Gesichtsanalyse: Schau mich an – und ich weiß, wer du bist" (translated: "Market research by facial recognition – look at me, and I know who you are"), published November 17th 2011, http://www.spiegel.de/netzwelt/netzpolitik/marktforschung-per-gesichtsanalyse-schau-mich-an-und-ich-weiss-wer-du-bist-a-797683.html

[212] Cf. Federal Trade Commission report of October 2012 "Facing Facts –- Best Practices for Common Uses of Facial Recognition Technologies", p. 3, http://ftc.gov/os/2012/10/121022facialtechrpt.pdf; see also Stephen D. Fried, CSSIP, "Enhancing Security through Biometric Technology", Chapter 1 in "Handbook of Information Security Management", published by Micki Krause, Harold F. Tipton, 5th edition, 2004, p. 7

[213] Emil Protalinski, TheNextWeb article, "The FBI pours $1 billion into facial recognition technology project, going nationwide in 2014", http://thenextweb.com/insider/2012/09/07/the-fbi-pours-1-billion-facial-recognition-technology-project-going-nationwide-2014/

[214] Gus Hosein for Privacy International, article published May 12th 2011, "Council of Europe refuses to investigate biometrics privacy", available at: https://www.privacyinternational.org/blog/council-of-europe-refuses-to-investigate-biometrics-privacy

- HIDE (Homeland security, biometric identification & personal detection ethics)[215]
- RISE (Rising Pan European and International Awareness of Biometrics and Security Ethics)[216]
- TURBINE (TrUsted Revocable Biometric IdeNtitiEs)[217]

Another EU-funded research project worth mentioning is the 3D Face project, which aims at a further development of 3D face recognition technology and enabling privacy protection of the 3D biometric templates in the biometric processes.[218] But regardless of the current and emerging capabilities of facial recognition – in combination with comparison data from different sources, like publicly available data pools in social media and elsewhere – the technology has already become a tool of interest for security agencies seeking to further explore its usage potential.[219]

State of technology

All biometric systems have generally common functional components. The starting point is the measurement of the bodily characteristic or trait to provide a biometric sample, which is then used to create a template file.[220] Then, this template may be used for several possible purposes, such as matching it with a comparison image. Depending on this purpose, it may be necessary to repeat the template creation process temporarily to enable a matching with the results of the initial process.

The typical model of such a measurement process encompasses three different stages, which are:

- Enrolment
- Template creation
- Matching

The enrolment is the input of the components for the personalisation or registration of individuals into the system. This means that a digital image of an individual's face is being fed into the system to provide the biometric information. Such an image may be either provided as an already existing file, or created specifically for this purpose by a sensor integrated into a biometric capture system. Often, the image is created using the footage of a CCTV camera (see Figure 8), whereby it is possible to capture the individual unknowingly and/or unwillingly.[221] The system analyses the visual information the image provides and evaluates if facial structures may be recognisable. If this is the case, the system then evaluates the recognised features of the face. One possibility is to measure the location of and distances between focal points, e. g. eyes, eyebrows, nose, mouth and chin. More advanced and complex 2D facial recognition systems use a so-called Eigenface and Multi Component Analysis approach, which is not restricted to few focal points such as eyes, mouth and nose. Rather, a pre-extracted face image onto a set of face space is used to be matched against an existing face data base for determining relevant

[215] http://www.hideproject.org/
[216] http://www.riseproject.eu/
[217] http://www.turbine-project.eu/
[218] http://www.3dface.org
[219] For example in the U.S., the aforementioned FBI's project NGI foresees the matching of facial recognition data with those to be found in public datasets to conduct automated surveillance. The EFF interprets these plans as an intention to be able to search and identify individuals people in crowd photos as well as in pictures posted on social media websites, cf. Jennifer Lynch for the Electronic Frontier Foundation, "FBI's Facial Recognition is Coming to a State Near You", article published August 2nd 2012, https://www.eff.org/deeplinks/2012/07/fbis_facial_recognition_coming_state_near_you
[220] Margaret Rouse, "Biometric Terms: Glossary", http://whatis.techtarget.com/reference/Biometric-Terms-Glossary
[221] Cf. Lucas D. Introna, Lancaster University, UK; Centre for the Study of Technology and Organization and Helen Nissenbaum, New York University; Department of Media, Culture, and Communication, "Facial Recognition Technology – A Survey of Policy and Implementation Issues", pp. 12 f., report created for the Center for Catastrophe Preparedness & Response, New York University July 22nd 2009

differences to known face images.[222] But regardless of which focal points of the face are used, other factors also play a role in conducting the recognition process: So, the location of the camera, i. e. the capture angle, is important to enable the adequate capture of all relevant parts of the face. Moreover, the processing algorithm must be able to perform the fractionation of the face into the relevant focal parts. In case thermal imaging cameras are used, they would be able to capture the warmth pattern of the vascular system under the individual's skin, allowing not only conclusions regarding the facial structure, but also body temperature and emotion of the subject.[223]

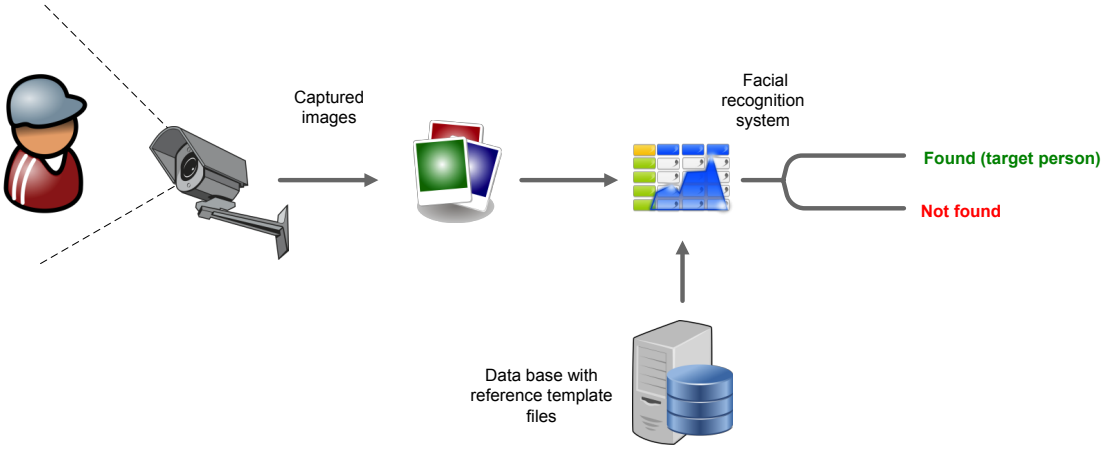

Figure 8: Facial recognition process, checking against a data base of target persons[224]

The results of the recognition enrolment will be transformed into a vectorised image[225] to form the template file information. This template may then be stored as a reference file in a data base to be used in follow-up processes for matching comparison images.[226] The matching process finally compares the stored template to the data set which is captured at a repeated enrolment process in the biometric system. As already mentioned above, the ISO distinguishes between two possible application areas of biometric recognition technologies. These are:

- Verification of an identity (also known as authentication)
- Identification of an individual

The verification process, as already mentioned before, performs the presentation of an already known individual's face to verify a claimed identity during the comparison with an existing template. This is a process used for physical access control in buildings or other areas with restricted access. This process may also be used for virtual access control linked to digital systems or assets. The verification process is also often called 'one-to-one comparison' as a

222 Abhishek Singh, Saurabh Kumar, "Face Recognition using PCA and Eigen face approach", BTech thesis published 2012, http://ethesis.nitrkl.ac.in/3814/1/Thesis.pdf

223 Kropatsch, Sablatnig, "Biometrics", p. 12; see also Francine Prokoski, "History, Current Status, and Future of Infrared Identification", pp. 5-14 for an overview of thermal imaging/infrared techniques for facial recognition.

224 Simplified model after P. Jonathon Phillips, Patrick Grother, Ross Micheals, Duane M. Blackburn, Elham Tabassi, Mike Bone, "Face Recognition Vendor Test 2002", DARPA et al., Arlington 2003

225 Introna/Nissenbaum, pp. 16 f.

226 Moritz Karg, "Biometrische Verfahren zur Gesichtserkennung und Datenschutz in Sozialen Netzwerken" (translated: "Biometric processes for facial recognition and privacy protection in social networks"), article for issue 7/2012, Humboldt Forum Recht, pp. 120 ff., http://www.humboldt-forum-recht.de/media/Druckansicht/pdf/2012-07.pdf

'*process in which biometric probe(s) from one biometric data subject is compared to biometric reference(s) from one biometric data subject to produce a comparison score*'.[227]

The identification process is more complex, whereby the biometric data enrolled is matched against a whole set of templates in a gallery. This 'one-to-many search' is defined as a

'*process in which a biometric probe(s) of one biometric data subject is searched against the biometric references of more than one biometric data subject to return a candidate list or comparison decision*'.[228]

There, it must be differentiated between so-called 'closed-set' and 'open-set' recognition processes. Closed set processes perform a matching whereby it is known that the individual sought must be in the template data base. In contrast, open-set processes perform the matching where it is not known whether the desired data set can be found in the template gallery.[229] However, Introna and Nissenbaum refer to a third application area for a data matching within a facial recognition system, called 'Watch list'. The watch list should involve a specific case of an open set identification task within a one-to-many-search which is executed in two steps: First, the system aims at determining if the new sample image matches a data set on a predefined watch list. In the second step, the system subsequently performs an identification of the individual.[230]

Whichever the specific preconditions of the process, once a match can be determined, the biometric recognition system signals the recognition of the individual. To illustrate the outcome of the matching process adequately, results are catalogued into different possible categories, which are vendor-dependent called differently. Some vendors name the possible results under specifically named labels such as false accept rate (or false match rate), false reject rate (or false non-match rate), additionally taking into account relative operating characteristics (defining the thresholds of the underlying algorithm), error rates and capture/enrolment failure rates.[231] Other vendors categorise differently. Also common is a categorisation using other labels such as True Negative, False Positive, False Negative, and True Positive (see Table 2).

		Reference template data base	
		Other person	Target person
Captured image (e. g. from video footage)	Other person	True Negative	False Positive
	Target person	False Negative	True Positive

[227] Cf. ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV), definition no. 37.05.10
[228] Ibidem, definition no. 37.05.12
[229] Introna/Nissenbaum, p. 12
[230] Ibidem, p. 13
[231] Stephen D. Fried in "Handbook of Information Security Management", pp. 8 ff.

Table 2: Example of a biometrics matching result schema in a one-to-many search process[232]

The above-described process is considered to be a classic 2D facial recognition process. However, this approach may under circumstances provide only accurate results when the enrolment processes occur under the very same circumstances to produce comparable image files. 2D systems are especially prone to errors under difficult or simply varying light conditions, or different capture angles during enrolment (more details to be found below in the section 'Effectiveness of facial recognition and civil right impact'). Due to these weaknesses of 2D facial recognition systems, R&D efforts of the last few years have concentrated on the development of 3D recognition processes taking into account the three-dimensional condition of the human face. This occurs in such a fashion that single focal points like eyes, mouth, nose, chin etc. are not simply captured and their distance to each other measured. Rather, all distances of the facial surface are measured, which may possibly require more than one capture image of the individual. The produced number of images from different angles will then be linked to each other. This way, 3D facial recognition systems produce a high-quality pixel-depth map of the facial structure, which can even be improved by adding information about the skin texture.[233]

Consequently, 3D recognition processes are far less affected by differing lighting settings during enrolment processes, although not completely unaffected. The fact that individuals never present themselves in exactly the same position and angle to the camera becomes mostly irrelevant since the processing of the scan occurs at an early step and each image is calibrated to provide unified footage for the following recognition process.[234] Also in contrast to 2D recognition, colour information is more often captured during the enrolment to optimise the pixel-depth visualisation of the facial features.[235]

Effectiveness of facial recognition and civil rights impact

Regardless of the societal impact of the technology in the context of security, the question is how effective from a technological point of view facial recognition can be. The core techniques of facial recognition have been subject to ambitious R&D efforts throughout the years to achieve further improvements regarding matching results. So far, these efforts still have provided unsatisfying results. Back in 2009, it was claimed that facial recognition technology deployed at Manchester airport could not distinguish the faces of the actress Winona Ryder and Osama Bin Laden owing to the fact that the device calibration signalled a match at a rate of only 30 percent likeness.[236] Also in 2009, the survey conducted by Introna and Nissenbaum found that the accuracy of facial recognition results has significantly improved, yet the performance of the system is still dependent on factors such as deployment environment, image age, consistent camera use, and template gallery size.[237] Mostly, it can

[232] Table roughly based upon the depiction of the result schema in the PPT presentation "Video Surveillance, Biometrics, and Privacy After 9-11" held in 2002 by Kevin Bowyer, Computer Science & Engineering University of Notre Dame.

[233] Image source: Kevin W. Bowyer, Kyong Chang, Patrick Flynn, "A survey of approaches and challenges in 3D and multi-modal 3D + 2D face recognition", p. 2, published online at ScienceDirect.com, Computer Vision and Image Understandingin , issue 101 (2006), pp. 1-15

[234] This step is also often called "normalization" which the Article 29 Working Party in its document "Opinion 02/2012 on facial recognition in online and mobile services" (WP 192), adopted March 22nd 2012 defined as the "process to smooth variations across detected facial regions, e. g. converting to a standard size, rotating or aligning colour distributions" see p. 2. The Article 29 Working Party was established due to the requirement of Article 29 EU Data Protection Directive 95/46/EC, which stipulated a working group "on the Protection of Individuals with regard to the Processing of Personal Data". The group has the function of an independent advisory group counselling the European Commission with respect to data protection and privacy issues.

[235] Bettina Otten, "3D Gesichtserkennung – Merkmalsdetektion in 3D-Scans und merkmalsbasierter Vergleich von Gesichtern" (translated: "3D facial recognition – trait detection in 3D-scans and trait-based comparison of faces"), pp. 24 ff., dissertation at the University Koblenz Landau, March 2006

[236] See Duncan Gardham in The Telegraph, published April 5th 2009 "Airport face scanners 'cannot tell the difference between Osama bin Laden and Winona Ryder" http://www.telegraph.co.uk/news/uknews/law-and-order/5110402/Airport-face-scanners-cannot-tell-the-difference-between-Osama-bin-Laden-and-Winona-Ryder.html

[237] Lucas D. Introna, Helen Nissenbaum, pp. 3 f.

be said that the capture, evaluation, and comparison of biometric characteristics and traits may be under circumstances faulty owing to measurement errors. These errors may be caused by age-dependent changes of the individual's appearance, but also by external influences like injuries or illnesses. Moreover, temporary changes of the appearance like hairstyle, beard, glasses, contact lenses or make up may significantly influence the outcome of the matching process. So it can be said that the following changes in appearance are influential to the accuracy of the measurement process:

- Aging
- Beards
- Glasses & contact lenses
- Make up
- Facial expression
- Light setting during capture

Furthermore, during an enrolment, the characteristic or trait will never be presented exactly in the same way by the individual. An example would be the slightest different angle to capture a face during the recognition process. So it can be said that two digital captures of a biometric trait will never be exactly the same.[238] The factual result of match or non-match will be decided by a process of 'similarity test' with prior configuration settings or parameters permitting a tolerance range of unlikeness. Consequently, certain biometric systems will only be able to decide with a system-inherent probability score if the captured individual is the targeted one.[239] 3D facial recognition systems have partly been able to overcome the similarity obstacle. However, current research is yet trying to resolve issues of illumination variation and sensor sensitivity to reduce error rates. Similarly, thermal imaging cameras are still prone to errors owing to environmental settings and the production of fairly low-resolution images. [240] Scientific research is currently focusing on new types of so-called adaptive recognition systems, which have an implemented auto-update function to track image variations for template creation. It is yet to be seen how effective these novel approaches prove to be.[241]

Though biometrics as unalterable characteristics may provide some protection against certain crimes like unauthorised access (e. g. to areas and devices where personal data bases are located) or identity theft, this specific feature of the technology may also cause privacy concerns.[242] According to the Article 29 Working Party,

> *'Biometric technologies are closely linked to certain characteristics of an individual and some of them can be used to reveal sensitive data. In addition many of them allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high. This impact is increasing through the growing deployment of these technologies. Every individual is likely to be enrolled in one or several biometric systems.'*[243]

---

238 German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), "Grundsätzliche Funktionsweise biometrischer Verfahren" (translated: "Basic functionality of biometric processes"), https://www.bsi.bund.de/ContentBSI/Themen/Biometrie/AllgemeineEinfuehrung/einfuehrung.html

239 Cf. David Moss, The Register, August 14th 2009, "Collar the lot of us! The biometric delusion – Optimism beats evidence in the drive to fingerprint the world", www.theregister.co.uk/2009/08/14/biometric_id_delusion/, elaborating about the high false matching rates of biometric systems deployed in the U.S. at that time.

240 Bowyer/Chang/Flynn, p. 10

241 Cf. Ajita Rattani, "Adaptive Biometric System bas*ed on Template Update Procedures*", p. 37, Ph.D. thesis at the University of Cagliari, Department of Electrical and Electronic Engineering, 2010

242 Cf. UK Communications-Electronics Security Group, website information "Privacy issues and biometrics" http://www.cesg.gov.uk/policyguidance/biometrics/Pages/MS06-Privacy-Issues.aspx

243 Cf. Article 29 Working Party, "Opinion 3/2012 on developments in biometric technologies" (WP 193), adopted on April 27th 2012, p. 3, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf;

One very crucial concern regarding facial recognition technologies is function creep: in other words, the inherent potential of exceeding data collection beyond the originally intended scope by the digital capture of the biometric traits. Depending on the system pre-configuration and algorithms used, the facial physiognomy allows for conclusions regarding age, gender, ethnic origin or even health status of the person. The last two traits especially belong to the category of sensitive personal data, whose processing may occur only under specific legal preconditions. Also, the collection of ethnicity data in particular triggers some risk potential regarding racial discrimination issues. Generally, the full extent of possible predications is not always transparent to the individual and is highly dependent on the type of deployed technology and the quality of enrolment, templating and matching processes. Concerned individuals are generally not able to assess the risks of such a data collection in a field where relevant characteristics are scarcely alterable.

This raises another concern, which is the creation and use of an unalterable and unique digital biometric reference set related to an individual. Note that because of interoperability reasons the required facial photo for eIDs such as the ePassport is optimised for biometric purposes and stored in a graphics format instead of transforming it into a template or using a specific biometric encryption. The biometric reference set can potentially be used anytime to identify the individual in question and combine it with additional data related to that person. Consequently, biometric data can form a tight connection or linking point for any kind of profiling, making it even more important to process and store the personal data securely and within legal limitations.[244]

Potential Privacy by Design approaches

Regarding Privacy by Design in biometrics, some research steps have been taken to explore the potential in this field of technology. Some core factors to enhance privacy in biometrics were mentioned at the TURBINE workshop in 2011, namely – as it is common for Privacy by Design approaches – data minimisation, maximum individual control, and improved security. While proposing these factors, an emphasis was made that the retention of biometric images shall be limited to minimise the potential for unauthorised secondary uses, loss, or misuse. Function creep shall be avoided and adequate methods for authentication, communication and data security shall be established. In the context of these data security enhancing measures, templates stored in data bases shall be encrypted sufficiently.[245] The EU-funded research project TURBINE (TrUsted Revocable Biometric IdeNtitiEs developed some best practices to protect the privacy of individuals. These are:

- Biometric data shall in principle only be used for verification
- User control over biometric data by default
- Multiple identities and pseudonymity
- Revocability of biometric identities and re-issuance
- Credential and/or identity check
- Deletion of the samples and of the original templates
- The use of privacy-enhancing technologies
- Transparency and additional information for the data subjects
- Specification of fall-back procedures and of the procedure to appeal a comparison decision

---

see also Article 29 Working Party, "Working document on biometrics" (WP 80), pp. 3 f., adopted on August 1st 2003, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf

244 Cf. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, "Privacy and Biometrics", p. 2 (1999), and Moritz Karg, "Biometrische Verfahren zur Gesichtserkennung und Datenschutz in Sozialen Netzwerken", p. 123

245 Michelle Chibba, Director of Policy and Special Projects at the Information and Privacy Commissioner's Office in Ontario, Canada, proposals mentioned in her presentation "Biometric Encryption: A Privacy by Design Example for Achieving Citizen Trust" held at the final workshop themed "CryptoBiometrics for Enhanced Trusted ID Management: Dreams & Reality" conducted by the research project TURBINE January 2011

- On the organisation (especially enrolment phase), the security and the certification of biometric IdM system[246]

However, some of these endorsed best practices are only applicable in the field of civil use of biometrics. Whenever biometrics are used for governmental surveillance purposes, in particular the question of what level of control the individual can exercise over his data becomes relevant. It is deemed important that at least the aspects of transparency and additional information should receive greater attention. Moreover, some of these best practices cover not only technological solutions, but also organisational measures, providing not as strong safeguards for the privacy of individuals as a privacy-enhancing measure directly built into the system. Still, according to the European Data Protection Supervisor (EDPS) Peter Hustinx, these best practices form a usable basis to review biometrics systems critically to explore their need of Privacy by Design implementations. Furthermore, the EDPS proposed general criteria for Privacy by Design in biometrics. These are:

- Targeted impact assessment taking into account relevant policies
- Emphasis on an accurate enrolment process with low False Rejection or False Acceptance rates
- Fall-back procedures in case an enrolment cannot be conducted[247]

Beyond these criteria, more tangible measures to enhance privacy directly triggered by the design of the system are decentralised data bases, evaluation and certification.[248] Further possible technical and organisational measures are:

- General enhancement of IT security as protection against data theft
- Protection against infiltration of foreign/inaccurate data, e. g. via electronic signatures of the reference templates
- Recognition of characteristics copies (anti-spoofing measure)
- Safeguarding the authenticity of the enrolment data, e. g. by supervision of staff present
- Logging of relevant processes and transactions[249]

Beyond these measures, research is also focusing on new techniques for so-called biometric template protection. Such techniques perform the creation of multiple references derived from the biometric data. These references will be created in such a way that they become unlinkable and non-invertible to secure the personal data inherent.[250] But whichever measure needs to be taken for the individual facial recognition system, what always must be considered is that the collection, processing and storage of personal data is only legitimate on the basis of legal grounds and within the boundaries of proportionality. For further details regarding the general legal preconditions in this context, see the corresponding project deliverable 3.2 (Report on regulatory frameworks concerning privacy and evolution of the norm of privacy).

---

246 Cf. TURBINE public deliverable R2.3 "Practical Guidelines for the privacy friendly processing of biometric data for identity verification" to be found at the project website www.turbine-project.eu

247 European Data Protection Supervisor Peter Hustinx, Opinion of February 1st 2011 on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development – Turbine (TrUsted Revocable Biometric IdeNtitiEs), available as PDF file at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf

248 UK Communications-Electronics Security Group, "Privacy issues and biometrics"

249 Cf. Whitepaper "Datenschutz in der Biometrie" (translated: "Data protection in biometrics"), pp. 19 f., TeleTrusT Deutschland e.V., Arbeitsgruppe Biometrie , Editors: H. Biermann, M. Bromba, C. Busch, G. Hornung, M. Meints, G. Quiring-Kock, Stand: 11.03.2008, available in German at: http://www.teletrust.de/publikationen/whitepapers/

250 Xuebing Zhou, abstract of the Ph.D. thesis at the Technische Universität Darmstadt, "Privacy and Security Assessment of Biometric Template Protection" (2012), available at: http://tuprints.ulb.tu-darmstadt.de/2885/

2.3.2 Body scanners

As introduced above, body scanners are not by definition a technology directly related to biometrics. However, as mentioned in the introduction of Chap2.3ter 2.3, they also concern bodily data and bodily integrity of individuals. The constant conflict between privacy and security is often at the core of public discussion, focusing on the fact that after the terrorist attacks of 9/11, Madrid and London[251], governments have increasingly deployed a variety of security measures. One of these measures is body scanners, a fairly new technology believed by experts able to guarantee security in a more efficient way than traditional methods are able to secure, e. g. aviation. This is believed to be so owing to the fact that the new-generation body scanners would be able to accurately detect liquids and non-metallic objects. But the introduction of these new scanner technologies is also heavily criticized for serious implications regarding data protection and privacy as well as regarding other fundamental rights of citizens. Nowadays these technologies are being implemented at a number of airports, with the U.S. perceived as the most intensely deploying nation, but some European countries following the example. This occurs partly with an already fixed establishment of body scanners and partly just with first tentative test runs. Already, security agencies consider the use of body scanner technologies helpful in securing not only airports, but also the entrances of public buildings, bus and train stations.

A full-body scanner is a device used to detect in a visual way any (forbidden) object which people may have (hidden) in their clothing or even (with X-rays) in their bodies. One difference between full-body scanners and conventional metal detectors is that this technology displays an image of the scanned individual without the clothing, in various levels of detail, depending on the device used. Due to that fact, some scanner types are considered very invasive with regard to privacy. Also, some scanner types may produce adverse health effects (see further elaborations below).

About the legal framework concerning body scanners, a Commission Regulation was issued in 2011 prohibiting the use of body scanners utilising ionising radiation at EU airports.[252] Another document related to body scanners is the Communication from the Commission to the European Parliament and the Council on the use of body scanners at EU airports.[253] This Communication analyses the use of body scanners, the technology, and the implications with regard to several fundamental rights, including privacy and data protection.

Body scanners are being implemented at airports all over the world.[254] Schiphol, in the Netherlands, was the first airport in the world to implement this device on a large scale after a test with flight personnel. On May 15th 2007, two of 17 purchased scanners were installed at this airport. Most of them have been installed in the United Kingdom (Manchester, Gatwick and Heathrow airports). The use of body scanners is compulsory in some countries, such as the United Kingdom, but, for example, in Ireland (Dublin airport), the use is optional. Also, some countries outside the European Union, such as the United States and Canada, have installed them in their respective airports. At the end of 2012, Australia started to use them in several airports (Adelaide, Brisbane, Cairns, Darwin, Gold Coast, Melbourne, Perth and

---

[251] These refer to the terroristic attacks of September 11th 2001 in New York, March 11th 2004 in Madrid, and July 7th 2005 in London.

[252] Commission Regulation (EU) No 1141/2011 of 10 November 2011 amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, see paragraph (5)

[253] Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports COM (2010) 311 of June 15th 2010, available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0311:FIN:EN:PDF

[254] A longer list of airports with full-body scanners can be found on: http://www.proyectoescaner.org/aeropuertos-con-escaneres-corporales/

Sydney).[255] Moreover, body scanners could be installed in other public buildings, such as railway stations, bus and ferry terminals[256], and even police stations.[257]

However, some countries of the European Union have refused to use body scanners. For example, the Italian government had planned to install, all over the country, body scanners at all airports and train stations. But in September 2010, the plan to remove the scanners from airports was announced. This was due to the fact that they were considered 'slow and ineffective.' Therefore, the scanners were removed from the Italian airports after the tests carried out in Rome, Milan, Palermo and Venice.[258] In addition to that, Germany did not find a practical use for body scanners at its airports. After intensive tests carried out on more than 800,000 passengers between September 2010 and July 2011 at Hamburg airport, the German government decided not to deploy these scanners. According to the German Minister of Internal Affairs, the tests have shown that the body scanners are not reliable as they cause too many false alarms. However, in November 2012, another test run in order to use body scanners started at Frankfurt airport.[259]

State of technology

In the following, we will briefly describe the different techniques used to perform the main purpose of body scanners, to detect liquids and other prohibited objects under the clothing of persons. The European Commission distinguishes between four different types of body scanners technologies:[260]

- Passive millimetre waves
  - The image is generated by the natural radiation of millimetre waves emitted by the body or reflected by what surrounds it. The main advantage of this technology is the absence of radiation. The main disadvantage lies in the fact that the body images are very elementary and fuzzy. However, hidden objects (metallic and non-metallic) are shown.

- Active millimetre waves
  - The body is illuminated by means of reflected short-wave radio waves to generate the image. This technology works on frequencies between approximately 30 and 300 GHz. This system has two advantages: the images created are high resolution so any object will be seen, and the surface of the body is shown in detail.

- X-ray backscatter
  - The backscattered radiation illuminates the body with low-dose X-rays to create a two-dimensional image of the body.

- X-ray transmission imagery
  - This technology also uses X-rays to produce images. In contrast to the aforementioned technique, these rays penetrate the clothing and body similar to the X-rays used in

[255] Cf. the website information of the Australian Government, Department of Infrastructure and Transport, http://travelsecure.infrastructure.gov.au/bodyscanners/index.aspx

[256] TheTransportation Security of Administration of United States (TSA) is considering installing them in such places, as certain documents released under the Freedom of Information Act have shown, cf. the article by Steve Watson at Prisonplanet.com, "More New Documents Show TSA Intends To Deploy Body Scanners At Rail, Bus, Ferry Terminals", September 7th 2012, http://www.prisonplanet.com/more-new-documents-show-tsa-intends-to-deploy-body-scanners-at-rail-bus-ferry-terminals.html

[257] Cf. Chris Alcantara, "Body scanner gives jail inside view of criminals", January 7th 2013, http://www.alligator.org/news/local/article_e8b4130a-5886-11e2-9b0c-001a4bcf887a.html

[258] The Sydney Morning Herald, article of September 24th 2010, "Italy to abandon airport body scanners", http://www.smh.com.au/travel/travel-news/italy-to-abandon-airport-body-scanners-20100924-15pgu.html

[259] http://goodtechsystems.com/from-now-on-body-scanners-at-frankfurt-airport/

[260] Taken from the descriptions provided in COM (2010) 311, pp. 8 f.

medicine for detecting metallic or non-metallic objects which have been swallowed or introduced into body cavities.

These four technologies have been tested at different airports for several years in order to evaluate their advantages and disadvantages. These tests occurred to lay the foundations for the decision over their possible introduction in order to improve security in the aviation environment. Considering the technologies introduced above, the most used nowadays are based on active millimetre waves and on X-ray backscatter. X-ray backscatter was very extensively used by the United States and the United Kingdom. However, just recently, the U.S. Transportation Security Administration (TSA) decided to lay off the use of full-body X-ray scanners at seven major airports. Officially, this was decided owing to privacy concerns related to the imagery of nude individuals generated by these devices. But it is rumoured that the pull-out was in truth decided on due to health concerns.[261]

Due to the high doses of radiation emitted by X-ray transmission equipment, no use of this technology is foreseen in Europe. In the meantime, active millimetre waves are now being tested at Schiphol airport (Amsterdam) and at Charles De Gaulle airport (Paris). Currently, other body scanner technologies are emerging, some of them using active or passive non-ionising radiation. But none of them have been tested sufficiently yet. Here are some of the new technologies:[262]

- Imaging by active and passive submillimetre waves (also called terahertz waves)
- Thermal imaging by infrared
- Acoustic imaging
- Molecular analysis to detect explosives and drugs

The technologies using infrared radiation (active and passive terahertz wave imagery, thermal infrared thermal imagery and acoustic imagery) must fully comply with European Directive 2006/25/EC regarding the minimum health and safety requirements concerning the exposure of workers to risks arising from physical agents.[263] According to this Directive, the employer has to adopt measures in order to limit the levels of exposure to optical radiation to protect health workers. For example, employers have to implement technical measures like '*the use of interlocks or shielding*' to reduce the emission.[264]

Effectiveness of body scanners and civil rights impact

According to the Communication of the European Commission, the general tests carried out in laboratories and within the framework of the operating trials at airports in several countries were interpreted in such a way that the scanners tested provided reliable results. In this Communication, the Commission highlights that the new-generation of body scanners produces enhanced security through higher probabilities of liquid and non-metallic object detection in contrast to conventional metal detector arches. So the new body scanners may maximise the possibilities of detecting threats and offer a considerably greater prevention capacity. In addition to that, body scanners may allow passengers to pass through the checkpoints faster than with the aid of conventional scanners. This includes the inspection of a larger number of passengers in a shorter period of time. So the tests carried out would show that it takes about 20 seconds to produce and interpret the relevant passenger data.

---

[261] The Associated Press, article of October 25th 2012 on CBS News, "TSA quietly removing some full body scanners" http://www.cbsnews.com/8301-201_162-57540714/tsa-quietly-removing-some-full-body-scanners/

[262] COM (2010) 311, p. 9

[263] Directive 2006/25/EC of the European Parliament and of the Council of 5 April 2006 on the minimum health and safety requirements regarding the exposure of workers to risks arising from physical agents (artificial optical radiation) (19th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC), http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:114:0038:0059:EN:PDF

[264] Article 5 para. 2 (c) of the Directive 2006/25/EC

In contrast to the view of the Commission, some tests and studies presented differing results regarding the effectiveness of body scanners. For example, L-3 low-level millimetre wave devices provided a quite high false alarm rate of 54 % during the test run at Hamburg airport, forcing the passengers to undergo additional pat-down security checks and leading to the termination of the test in July 2011. Similarly, the false alarm rates led to the termination of the test runs executed at the Charles de Gaulle airport in France in May 2010 and in Italy at the airports of Milan and Rome (false alarm rate of 23 %) in September 2011. These false alarms also occurred with similar scanners deployed at other airports, for instance in the U.S. Generally, it can be said that these false alarms were mostly triggered by:

- Folds in clothing
- Buttons
- Sweat/perspiration spots

This is due to the fact that these millimetre wave scanners react to fluids as they penetrate clothing materials differently, leading the erroneous alarms whenever several layers of clothing form a barrier for the screening process. Interestingly, X-ray scanners of Rapiscan Systems used at Manchester airport in the UK produced a false alarm rate of just 5 %.[265] Beyond these faults of the technology, it is also possible to actively trick the scanners to smuggle prohibited fluids and objects through the security check. For example, in March 2012, blogger Jonathan Corbett proved this by a demonstration executed at various airports using both X-ray as well as millimetre wave scanners. He showed in video footage how to get past the scanners by using specific clothing with hidden pockets to avoid metallic objects being shown on the display imagery of the scanner. This demonstration on how to effectively render the body scan useless went viral; still the TSA denied its validity.[266]

Health matters that must be taken into consideration are different according to the technology used. The applicability of the legal framework depends on the technologies used owing to the fact that some devices do not utilise radiation at all, while others expose scanned persons to varying doses of radiation. Diverse European and international studies[267] have been conducted on security aspects of body scanners or the technologies underlying these (for example, exposing people inspected, operators and other people who are working with the machines or next to them to radio waves and ionising radiation). Although there are several research documents related to the general impact of these technologies on the human being, we will here concentrate more on the studies that have investigated the effects in the

[265] Michael Grabell, Christian Salewski, "Sweating Bullets: Body Scanners Can See Perspiration as a Potential Weapon", December 19th 2011, www.propublica.org/article/sweating-bullets-body-scanners-can-see-perspiration-as-a-potential-weapon

[266] Jonathan Corbett blog entry of March 6th 2012 with video footage and transcript: "1B of TSA Nude Body Scanners Made Worthless By Blog – How Anyone Can Get Anything Past The Scanners" ,http://tsaoutofourpants.wordpress.com/2012/03/06/1b-of-nude-body-scanners-made-worthless-by-blog-how-anyone-can-get-anything-past-the-tsas-nude-body-scanners/

[267] At European level see: Note of 15.2.2010, Agence Française de Sécurité Sanitaire de l'Environnement et du Travail relative au "Scanner corporel à ondes 'millimétriques' ProVision 100", The French Institute for Nuclear Radioprotection and Safety (IRSN), "Evaluation du risque sanitaire des scanners corporels à rayons X «backscatter", rapport DRPH 2010-03 and Recommandations 2007 de la Commission Internationale de Protection Radiologique, ICPR 103; Health Protection Agency, Centre for Radiation, Chemical and Environmental Hazards (HPA), UK, "Assessment of comparative ionizing radiation doses from the use of rapiscan secure 1000 X-ray backscatter body scanner", UK January 2010, available at: http://webarchive.nationalarchives.gov.uk/20111005131753/http://www.dft.gov.uk/publications/assessment-of-comparative-ionising-radiation-rapiscan-security-scanner).
For international studies, see: The American Interagency Steering Committee on Radiation Standards (ISCORS), "Guidance for Security Screening of Humans Utilizing Ionizing Radiation Technical report 2008-1" The National Council on Radiation Protection and Measurement (NCRP), "Commentary 16 – Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems" (2003) and International Commission on Non-Ionizing Radiation Protection (ICNIRP), "Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields" (1998); 2010 Report by the Inter-Agency Committee on Radiation Safety on scanners (non-public report).

case of scanners used in aviation protection. According to experts, the use of X-ray body scanners can in particular cause negative consequences for health.[268] This mostly concerns the airport security staff responsible for the maintenance of the scanners.[269] These concerns led to the prohibition of scanners with ionising radiation in the EU in 2011.[270] In the U.S., the Inter-Agency Committee on Radiation Safety interfered with its report to the concerned agencies, stating that no pregnant women and children should be scanned and exposed to radiation, even if the dose is low.[271] In 2012, the U.S. TSA started to review the safety of X-ray body scanners after evidence of increased cases of tumour diseases affecting TSA agents at Boston Logan Airport.[272] Moreover, the U.S. National Academy of Sciences was tasked with conducting an independent assessment of airport body scanners in December 2012.[273]

Beyond the effectiveness and health issues, body scanners were also criticised owing to their negative impact on human rights, especially with regard to human dignity, privacy and data protection. This mostly concerns the X-ray body scanners displaying full nude imagery of the screened individuals. These scanners were perceived as very intrusive and humiliating by the public and became a topic of heated discussion regarding their necessity. Beyond this fact, a former TSA agent claimed that security employees at the airport being tasked with the observation of the scanner displays made fun of nude images of passengers. The Agency itself denied that claim.[274]

Also, the use of body scanners may under circumstances reveal the health status of the individual undergoing the screening, for example, if the person has a prosthesis. Data collected by these scanners are personal data by definition of the Article 29 Working Party.[275] Among other data types, health data especially is considered highly sensitive personal data, for which specific legal preconditions must be fulfilled to render the collection, processing and storage lawful. So airport security operators have to comply with a number of general principles and duties of data protection: transparency, consent of data subject, security measures, and legitimate purpose.[276] There might also be people who find it difficult to reconcile their religious beliefs with a procedure in which their body image has to be examined by an inspector. In this context, especially Muslim women may be affected. Likewise, in application of the right to equality and prohibition of discrimination, it is necessary for the operating rules to guarantee that passengers asked to pass through a body scanner are not chosen according to their sex, race, colour, ethnic or social origin, religion or beliefs. Also, special considerations should be made for minors, disabled and elderly people.

---

[268] COM (2010) 311, p. 16

[269] Cf. Wendy Thomson, elaborating about the doses of radiation the employees are exposed to on the TSA News Blog, "Ignore the man behind the curtain", February 29th 2012, tsanewsblog.com/1750/news/ignore-the-man-behind-the-curtain/

[270] Cf. Commission Regulation (EU) No 1141/2011 of 10 November 2011

[271] Jonathan Tirone for Bloomberg, "Airport Body Scanning Raises Radiation Exposure, Committee Says", February 5th 2010, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aoG.YbbvnkzU&pos=11

[272] Paul Joseph Watson for Prisonplanet.com, "TSA To Test Body Scanner Operators For Radiation Exposure", January 16th 2012, http://www.infowars.com/tsa-to-test-body-scanner-operators-for-radiation-exposure/

[273] See News section entry on the website of the Electronic Privacy Information Center (EPIC) of December 19th 2012, "National Academy of Sciences to Undertake Independent Assessment of Airport Body Scanners", http://epic.org/2012/12/national-academy-of-sciences-t.html

[274] Hugo Martin, Los Angeles Times, "Are TSA officers laughing at you? Agency says no", January 6th 2013, http://www.latimes.com/business/la-fi-mo-tsa-officers-laughing-20130103,0,1200411.story

[275] According to both the Article 29 Working Party documents WP 193 on biometrice (pp. 3 f.) and the "Opinion 4/2007 on the concept of personal data" (WP 136), adopted June 20th 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
However, outside Europe, this assessment may differ. In Australia, the screening images of individuals are not considered personal data because "*No identifying information such as names, passport numbers or flight details is collected, used or disclosed during the process of undertaking a body scan*", p. 25, see *"The use of body scanners for aviation security screening in Australia: Privacy Impact Assessment"* published by the Australian Government, Department of Infrastructure and Transport in February 2012.

[276] Cf. the Directive 95/46/EC of the European Parliament and of the Council, of 24th October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Potential Privacy by Design approaches

So-called 'Privacy by Design' and privacy protection technologies applied to the design of body scanners may reduce the negative impact regarding data protection and other civil rights, e. g. by choosing a technology less intrusive to privacy instead of using technology that shows people naked.[277] Some first steps have been taken in Europe by a broader deployment of mostly millimetre wave body scanners displaying only an outline of the body and highlighting only suspicious objects.

Images should not be stored, or should be deleted at the latest when the person has left the control point, except if the person has been retained for having a prohibited article. In this last situation, the images should be deleted when the person is allowed to continue or security staff must deny access.[278] The possibility of adopting high security measures in order to guarantee the protection of the personal data should be evaluated. Related to these kinds of security measures the following criteria must be taken into account:

- The possibility of recording health data
- Biometric data in Central & North European Union are considered, in some countries, to be sensitive data
- One of the high-security measures is the auditing of the data base, as we consider that body scanners are more invasive with regards to data subject privacy than normal scanners, so the system should be audited every two years[279]
- If the security measures are high, the transfer of images, for example addressed to police, should be encrypted[280]

The images should be viewed and controlled in a room separate from the machine. This measure prevents the rest of the passengers from viewing the body scanner images; only people responsible for monitoring the scanners will be able to view the images.[281] Moreover, the possibility to appoint a responsibility for security should be evaluated.[282] Also, it would be possible to distinguish between employees directly involved with the observation and maintenance of the scanners and those who are tasked with management duties, who are most likely to decide about the communication to the police in case of a security incident.

2.4 Data matching, linkage & analysis

All of these above-described technologies have one thing in common: they can provide information to security agencies. However, in the wake of such data collection, processing and storage, personal data of individuals are involved. While the functionality focus of some of these technologies may target certain individuals, there are others that perform their functions on a broader scope, for instance Smart CCTV, drones or cell tower data dumps, capturing data from a wide range of applications or settings. Often, the respective technology provides no opportunity for a prior data collection limitation to a predefined target group of suspected criminals. Moreover, digital capturing devices have in recent years

[277] Recently, the United States has started to replace this kind of scanner, see article in El Pais of January 18th 2013, "EEUU retira los escáneres de los aeropuertos por sus imágenes explícitas", http://tecnologia.elpais.com/tecnologia/2013/01/18/actualidad/1358517550_531128.html

[278] According to Instruction 1/2006 issued by the Spanish Data Protection Agency of Surveillance, the maximum term of data retention for a body scanner image is one month which seems to be quite long.

[279] Royal Decree 1720/2007 of Data Protection (Spanish Legal Framework) established as high security measure the auditing of databases every two years.

[280] Royal Decree 1720/2007 of Data Protection (Spanish Legal Framework) established as high security measure the encryption of personal data (sensitive data) when you send them.

[281] Cf. the suggestions made in the Privacy Impact Assessment conducted by the Department of Infrastructure and Transport of Australia in February 2012.

[282] Royal Decree 1720/2007 of Data Proteccion (Spanish Legal Framework), regulating the responsibility of security for medium and high security measures.

become increasingly efficient, providing vast amounts of data input to be counted in terabytes, petabytes and exabytes. Ultimately, this leads to a challenge of the modern ICT world, which is to sift out useful information from such a flood of data – and to limit the use of it to legitimate purposes and adhere to the proportionality principle. Not only is storage space, therefore, an issue, but also means of data protection and privacy as well as the proliferation of the data. Because this concerns not only governmental use of data for security purposes, but also civil uses in all possible forms, the ICT industry is focusing strongly on new means of getting to grips with the issue. Accordingly, IBM, Oracle, SAP and Microsoft have invested over $15 billion in recent years to incorporate smaller startups specialised in data management and analytics.[283] These approaches to data management and analytics are also called Big Data – a concept mostly defined simply by the size, but sometimes also by the sheer complexity of the task at hand. Moreover, Big Data entails a number of different elements, such as:

- The degree of complexity within the data set
- The amount of value that can be derived from innovative vs non-innovative analysis techniques
- The use of longitudinal information supplements the analysis[284]

A 2011 McKinsey report explicitly mentions promising techniques which are deemed suitable to serve the purpose of Big Data. According to the report, these include data fusion and integration, association, rule learning, classification, cluster analysis, crowdsourcing, ensemble learning, genetic algorithms, machine learning, natural language processing, neural networks, predictive modelling, regression, sentiment analysis, signal processing, supervised and unsupervised learning, simulation, time series analysis, pattern recognition and anomaly detection, and ultimately, the visualisation of results.[285] Such techniques potentially relevant in the field of surveillance-oriented security technologies (SOST) are intensively explored by different research projects.

The most prominent example is the widely criticised EU-funded project INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment)[286], which aims at developing automated algorithms for human decision support. Security-threatening challenges like terrorism, human trafficking, child pornography, the detection of dangerous situations (e. g. robberies), and the use of dangerous objects (e. g. knives or guns) in public spaces are a strong focus of this project. Such projects build upon intensified R&D approaches of automated behavioural pattern & anomaly recognition processes. For instance, efforts are being made to enhance facial recognition systems in such a way that they become able not only to derive the facial features, but also to recognise and analyse the facial expressions made by the captured individuals.[287] Other algorithms are being worked on to read movements and actions of persons to identify threatening and violent behaviour by Smart CCTV.[288] But the most crucial weakness of such automated means of data

[283] Kenneth Cukier in an interview article for The Economist, "Data, data everywhere",February 25th 2010, www.economist.com/node/15557443

[284] Taken from the Big Data Definition website entry of MIKE2.0, the open source standard for Information Management, mike2.openmethodology.org/wiki/Big_Data_Definition

[285] James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers, McKinsey Global Institute Report, "Big data: The next frontier for innovation, competition, and productivity", published May 2011 and available as PDF file at: www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation

[286] www.indect-project.eu; but criticism does not limit itself to this project alone. Rather, issues around the project propositions of CleanIT and Horizon 2020 were also the subject of public discussion and concern of civil rights activists as well as data proitection & privacy experts, cf. Alexander Sander for Netzpolitik.org, "INDECT ist nur ein Symptom – EU-Forschung braucht effektive Kontrolle!" (translated: "INDECT is just a symptom – EU research needs effective supervision"), October 9th 2012, https://netzpolitik.org/2012/indect-ist-nur-ein-sympton-eu-forschung-braucht-effektive-kontrolle/

[287] Karen Weintraub for The New York Times, "But How Do You Really Feel? Someday the Computer May Know", October 15th 2012, https://www.nytimes.com/2012/10/16/science/affective-programming-grows-in-effort-to-read-faces.html?_r=2&

[288] Adi Robertson, "Military-backed surveillance prototype can read people's actions on video"

analytics is that they require stereotypical predefinitions and are not yet able to perform satisfying self-learning results.[289]

Whichever means of data analysis is chosen, the number and value of the results are strongly dependent on the sources of the information. Security-related data bases of the most different kind have increased significantly in the recent year. Popular examples to be mentioned are the Passenger Name Record (PNR) or the Advanced Passenger Information System (APIS) established in the field of aviation and border protection. Other approaches proposed by security agencies are advanced data bases for criminals[290] and terrorists[291] as well as the permission to share information among different agencies/institutions and internationally[292].

More information about European citizens like financial data[293], communication records[294], and DNA data bases shapes an even more comprehensive picture of their life. But what is often forgotten is that adequate analytics processes to cope with the influx of information are heavily dependent on the correctness of the data input used.[295] Moreover, there is a very real danger of so-called function creep by extensive profiling. This is well explained in the context of the Big Data Definition by MIKE2.0, the open source standard for Information Management, which states that the *'answer is in the number of independent data sources, each with the potential to interact. Big data doesn't lend itself well to being tamed by standard data management techniques simply because of its inconsistent and unpredictable combinations.'*[296] Therewith, privacy issues are inherent because sometimes the data collected and analysed may reveal more than was desired, the principle of purpose limitation is strongly violated, and contextual integrity cannot be kept. First steps towards a reasonable treatment of the technical opportunities at hand are just being made. So for example, restricting the access to the collected data and establishing transparency for concerned citizens are seen as critical factors in the field of Big Data.[297]

Finding even more solutions to the aforementioned issues will in the next few years become a big prospect for new research and development initiatives. It is yet to be seen how they will succeed in reining in groundless excessive data collections and still preserve the chances for providing security to citizens in the European Union.

---

289 For a more detailed explanation, see above in chapter "Smart CCTV" subsection "Effectiveness of Smart CCTV and civil rights impact"

290 For example in Germany, a database to track right wing extremism was established, see Sylvia Poggioli for NPR News, "With A Database, Germany Tracks Rise Of Neo-Nazis", October 11th 2012, http://www.npr.org/2012/10/11/162663914/with-a-database-germany-tracks-rise-of-neo-nazis

291 Also in the U.S., new databases are established, cf. Julia Angwin for Wall Street Journal, "U.S. Terrorism Agency to Tap a Vast Database of Citizens", December 13th 2012, http://online.wsj.com/article_email/SB10001424127887324478304578171623040640006-lMyQjAxMTAyMDEwMzExNDMyWj.html?mod=wsj_valettop_email#

292 For example, European member states strive for optimising the instruments for obtaining and analysing information. In doing so, they use joint undertakings, for example by Europol and Eurojust, cf. the website of the Summaries of EU legislation, information on Europe's counter-terrorism strategy, europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33275_en.htm

293 E. g. collected by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)

294 Josh Bell for the American Civil Liberties Union (ACLU), "VIDEO: NSA Whistleblower Explains How the U.S. Government Is Spying on Every Single Electronic Communication You Have", August 23, 2012, http://www.aclu.org/blog/national-security/video-nsa-whistleblower-explains-how-us-government-spying-every-single

295 Paul Ohm, Havard Business Review Blog Network, "Don't Build a Database of Ruin", August 23rd 2012, blogs.hbr.org/cs/2012/08/dont_build_a_database_of_ruin.html

296 mike2.openmethodology.org/wiki/Big_Data_Definition

297 Manyika/Chui/Brown/Bughin/Dobbs/Roxburgh/Byers, McKinsey Global Institute Report 2011, "Big data: The next frontier for innovation, competition, and productivity", pp. 5, 12

3 Observations & conclusions

In this document, we have described a number of selected technologies proposed as being useful for enhancing security within the European Union. We found technological progress from the military field, e. g. features of Smart CCTV or drones, led to systems that become increasingly used domestically, pushing the limits of privacy and civil rights. In the wake of the terrorist events of 9/11 and afterwards, governments across the globe set priorities to safeguard the security of their state. Thereby, debates were sparked about surveillance-oriented security solutions (SOSSs) skirting or even crossing the boundaries of constitutional principles and ethics. For some of such solutions, their human rights impact is already acknowledged, whereas for other solutions, policy-makers worldwide are still trying to decide over their acceptability for the sake of maintaining security and over the conditions that determine their usage.

In particular, the terrorist events instilled a fear of unexpected, hazardous violence worldwide, leading to a shift of perception and approach for security agencies. The necessary distinction between security as a subjective perception and real threats became blurred. Knowledge even slightly seen as relevant for countering security threats is increasingly sought to be obtained intelligence-driven, meaning that many means of surveillance occur covertly, often intransparently, even sidestepping supervision and accountability. Generally, states in the European Union have a well-balanced approach to manage democratic governance and the constitutional protection of their citizens. However, in trying to maintain security in Europe, member states have taken to surveillance practices in order to achieve this goal. This also means that security is increasingly sought to be achieved through means of technology, using the massive advancements the digital era has to offer.

We described the vast possibilities Smart CCTV and drones provide for observing public space areas, and we introduced to some very effective means of surveillance in the digital sphere. Moreover, surveillance technologies closely tied to the bodily integrity of individuals such as facial recognition and body scanners are also regarded as possible solutions by security agencies. Together with fairly new possibilities of making use of the data collected, for example by certain techniques in the context of Big Data, these technologies provide for ample opportunity to comprehensively scrutinise an individual's personal habits, beliefs, and life conditions. As a logical consequence, new dimensions of civil rights issues arise, making a more contextual view of security-oriented surveillance technologies urgently needed. The impact of such technologies on European citizens must be assessed closely, especially taking into account emerging technological capabilities and freshly inaugurated ways of data matching, linkage and profiling. Moreover, non-technical alternatives and legal safeguards as examined in the accompanying documents D3.2 and D3.3 need to be taken into account.

In this document, we found that the mere technical aspects of Privacy by Design are not always satisfying owing to the intrusive nature of some technologies. Drones and Deep Packet Inspection are illustrative, albeit not conclusive, examples of such poor chances of implementing PbD. Therefore, we propose that for such technologies specifically focused research should carefully examine their compatibility with the governance of a democratic state respecting the civil rights of its citizens. Further, the development of ICT architectures in general should follow the principle of Privacy by Design – the current state-of-the-art, e. g. of mobile telecommunication networks or of the Internet, shows deficiencies in implementing privacy principles. This renders it difficult to sketch out fully PbD SOSSs – here a Privacy-by-Redesign approach would be necessary that takes into account all democratic principles and prevents a surveillance state.

4 Bibliography

acatech, Deutsche Akademie der Technikwissenschaften, 'Internet Privacy', multidisciplinary analysis published by Johannes Buchmann, September 2012, www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Projektberichte/acatech_STUDIE_Internet_Privacy_WEB.pdf

Ackerman, Spencer, Wired.com, 'Air Force Keeps "Micro-Aviary" Of Tiny, Bird-like "Bots"', February 11th 2011, www.wired.com/dangerroom/2011/11/air-force-micro-aviary-drones/

ADDPRIV project, 'Deliverable 2.1: Review of existing smart video surveillance systems capable of being integrated with ADDPRIV project', Submission date July 31st 2011, www.addpriv.eu/uploads/public%20_deliverables/149–ADDPRIV_20113107_WP2_GDANSK_Scoreboard_R11.pdf

AFP article at Phys.org, 'Japan security firm to offer private drone', December 27th 2012, http://phys.org/news/2012-12-japan-firm-private-drone.html

AFP article in *The Sydney Morning Herald*, 'Japan to develop drones to monitor radiation', June 13th 2012, www.smh.com.au/technology/sci-tech/japan-to-develop-drones-to-monitor-radiation-20120613-208zs.html

AFP article in *The Sydney Morning Herald*, 'Italy to abandon airport body scanners', September 24th 2010, www.smh.com.au/travel/travel-news/italy-to-abandon-airport-body-scanners-20100924-15pgu.html

Alcantara, Chris, 'Body scanner gives jail inside view of criminals', January 7th 2013, www.alligator.org/news/local/article_e8b4130a-5886-11e2-9b0c-001a4bcf887a.html

Angwin, Julia, *The Wall Street Journal*, 'U.S. Terrorism Agency to Tap a Vast Database of Citizens', December 13th 2012, http://online.wsj.com/article_email/SB10001424127887324478304578171623040640006-lMyQjAxMTAyMDEwMzExNDMyWj.html?mod=wsj_valettop_email#

ARGUS-IS project (Autonomous Real-Time Ground Ubiquitous Surveillance-Imaging System), www.darpa.mil/Our_Work/I2O/Programs/Autonomous_Real-time_Ground_Ubiquitous_Surveillance-Imaging_System_%28ARGUS-IS%29.aspx

Arnold, Heinz, '130 Mio. intelligente Stromzähler bis 2016 in Europa' (2011), www.energie-und-technik.de/automatisierung/news/article/80591/0/130_Mio_intelligente_Stromzxxxaumlxxxhler_bis_2016_in_Europa/

Article 29 Working Party,
'Opinion 3/2012 on developments in biometric technologies' (WP 193), adopted on April 27th 2012,
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

'Opinion 02/2012 on facial recognition in online and mobile services' (WP 192), adopted on March 22nd 2012,
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

'Opinion 12/2011 on smart metering' (WP 183), adopted on April 4th 2011,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

'Opinion 4/2007 on the concept of personal data' (WP 136), adopted on June 20th 2007,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

'Working document on biometrics' (WP 80), adopted on August 1st 2003,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf

ATTAC Germany, 'Wie Deutschland lernt die Drohne zu lieben!', June 7th 2012,
lernt-die-drohne-zu-lieben/?cHash=6bd499163469d0d6cda13474da4b1b2d

Australian Government, Department of Infrastructure and Transport, 'The use of body scanners for aviation security screening in Australia: Privacy Impact Assessment', February 2012

Bankston, Kevin, Electronic Frontier Foundation, 'Surveillance Shocker: Sprint Received 8 MILLION Law Enforcement Requests for GPS Location Data in the Past Year', December 1st 2009,
https://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law

Barnes, J. B. and Cross, P. A., 'Processing Models for Very High Accuracy GPS Positioning', Journal of Navigation, 51, pp. 180-193; research paper conducted for the Department of Geomatics, Newcastle University and supported by the EPSRC and Trimble Navigation (1998),
www.gmat.unsw.edu.au/snap/publications/barnes_etal98a.pdf

BBC News South Asia, 'Drones: What are they and how do they work?', January 31st 2012,
www.bbc.co.uk/news/world-south-asia-10713898

Bedner, Mark, 'Rechtmäßigkeit der Deep Packet Inspection', analysis created for the 'Projektgruppe verfassungsverträgliche Technikgestaltung (provet)' at the Universität Kassel (2009),
www.kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf

Bell, Josh, American Civil Liberties Union (ACLU), 'VIDEO: NSA Whistleblower Explains How the U.S. Government Is Spying on Every Single Electronic Communication You Have', August 23, 2012,
www.aclu.org/blog/national-security/video-nsa-whistleblower-explains-how-us-government-spying-every-single

Booth, Robert, *The Guardian*, 'Government plans increased email and social network surveillance', April 1st 2012,
www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance

Bowcott, Owen and Hopkins, Nick, *The Guardian*, 'Future is assured for death-dealing, life-saving drones', August 4th 2012,
www.guardian.co.uk/world/2012/aug/04/future-drones

Bowe, Rebecca, Electronic Frontier Foundation, '2012 in Review: Biometric ID Systems Grew Internationally … And So Did Concerns About Privacy', December 29th 2012, https://www.eff.org/deeplinks/2012/12/biometric-id-systems-grew-internationally-2012-and-so-did-concerns-about-privacy

Bowley, Graham, *The New York Times*, 'Spy Balloons Become Part of the Afghanistan Landscape, Stirring Unease', May 12th 2012, www.nytimes.com/2012/05/13/world/asia/in-afghanistan-spy-balloons-now-part-of-landscape.html?pagewanted=all&_r=0

Bowyer, Kevin; Chang, Kyong; Flynn, Patrick, 'A survey of approaches and challenges in 3D and multi-modal 3D + 2D face recognition', published at ScienceDirect, *Computer Vision and Image Understanding*, issue 101 (2006),

Bowyer, Kevin, Computer Science & Engineering University of Notre Dame, PPT presentation 'Video Surveillance, Biometrics, and Privacy After 9-11' held in 2002 & available at: http://ssc.bibalex.org/viewer/detail.jsf;jsessionid=88452CF1F20EF67D90990F9945215494?lid=C7C5F4685C20BF640193CCF31EF67201&aterm=Search&page=146&tid=42880006BA7E264A8214C32947209C7A&atype=area&apage=1&id=2F96A3A57955C2A4307695F4D2C7D21D

British Electrotechnical and Allied Manufacturers Association (BEAMA) (Ed.), 'European Smart Metering Alliance – Final Report', p. 9. (2010)

Cavoukian, Ann, Information & Privacy Commissioner, Ontario, Canada, 'Privacy by Design – The 7 Foundational Principles', originally published: August 2009, latest revision December 2012: 'Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices', www.privacybydesign.ca

Cavoukian, Ann; Abrams, Martin E.; Taylor, Scott, 'Privacy by Design: Essential for Organizational Accountability and Strong Business Practices'

Chandler, David L., *MIT News*, 'Is that smile real or fake? A computerized system developed at MIT can tell the difference between smiles of joy and smiles of frustration', May 25th 2012, http://web.mit.edu/newsoffice/2012/smile-detector-0525.html

Chaos Computer Club Germany,
'Chaos Computer Club analyzes government malware', October 8th 2011, www.ccc.de/en/updates/2011/staatstrojaner;
'Chaos Computer Club analyzes new German government spyware', October 26th 2011, www.ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner;
'Analyse einer Regierungs-Malware', October 8th 2011, www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

Chibba, Michelle, Director of Policy and Special Projects at the Information and Privacy Commissioner's Office in Ontario, Canada, 'Biometric Encryption: A Privacy by Design Example for Achieving Citizen Trust', presentation held at the final workshop themed 'CryptoBiometrics for Enhanced Trusted ID Management: Dreams & Reality' conducted by the research project TURBINE January 2011

Choi, Charles, LiveScience, 'Tiny Drone Reveals Ancient Royal Burial Sites', October 7th 2011, www.livescience.com/16443-micro-drone-archaeology-burial-sites.html

Clauß, Ulrich, *Die Welt*, 'Bundespolizei erprobt Drohnen beim Küstenschutz' (translated: 'Federal police testing drones for coastal protection'), December 28th 2012, available only in German at:

www.welt.de/politik/deutschland/article112252357/Bundespolizei-erprobt-Drohnen-beim-Kuestenschutz.html

Cockrell School of Engineering of The University of Texas at Austin, 'Cockrell School Researchers Demonstrate First Successful "Spoofing" of UAVs', www.engr.utexas.edu/features/humphreysspoofing

Cole, Chris, Drone Wars UK, 'Drone Wars Briefing – Examining the growing threat of unmanned warfare', January 2012, www.dronewars.net

Cooper, Alissa, 'Doing the DPI Dance: Assessing the Privacy Impact of Deep Packet Inspection', in William Aspray, Philip Doty (Eds.), Privacy in America: Interdisciplinary Perspectives, 2011, pp. 139-165, http://www.alissacooper.com/wp-content/uploads/2011/10/DPIchapter.pdf

Corbett, Jonathan, '$1B of TSA Nude Body Scanners Made Worthless By Blog – How Anyone Can Get Anything Past The Scanners', with video footage and transcript, March 6th 2012, http://tsaoutofourpants.wordpress.com/2012/03/06/1b-of-nude-body-scanners-made-worthless-by-blog-how-anyone-can-get-anything-past-the-tsas-nude-body-scanners/

Croft, Neil J. and Olivier, Martin S., 'A Silent SMS Denial of Service (DoS) Attack', Southern African Telecommunication Networks and Applications Conference 2007 (SATNAC 2007) Proceedings (2007), http://mo.co.za/abstract/silentdos.htm

Cukier, Kenneth, interview for *The Economist*, 'Data, data everywhere', February 25th 2010, www.economist.com/node/15557443

Dapp, Thomas F., study commissioned by the Deutsche Bank, 'Growing need for security in online banking', published February 8th 2012

Davies, Simon G., Department of Law, University Of Essex, 'Assessing Biometrics and Privacy and Touching Big Brother – How biometric technology will fuse flesh and machine', published in *Information Technology & People*, vol 7, no. 4 (1994), https://www.privacyinternational.org/reports/assessing-biometrics-and-privacy-and-touching-big-brother

Defense Advanced Research Projects Agency (DARPA) of the U.S. Pentagon, 'Making Connections at 45,000 Feet: Future UAVs May Fuel Up In Flight', October 5th 2012, www.darpa.mil/NewsEvents/Releases/2012/10/05.aspx

Diehl, Jörg, *Spiegel Online*, 'Polizei-Drohnen: Himmelfahrtskommando für die Schönwetterspäher', June 22nd 2010, www.spiegel.de/panorama/polizei-drohnen-himmelfahrtskommando-fuer-die-schoenwetterspaeher-a-701310.html

Doward, Jamie, *The Guardian*, 'Crackdown on sale of UK spyware over fears of misuse by repressive regimes', September 9th 2012, www.guardian.co.uk/world/2012/sep/09/block-on-exports-surveillance-equipment

Electronic Privacy Information Center (EPIC), 'National Academy of Sciences to Undertake Independent Assessment of Airport Body Scanners', December 19th 2012, http://epic.org/2012/12/national-academy-of-sciences-t.html

El Pais, 'EEUU retira los escáneres de los aeropuertos por sus imágenes explícitas', January 18th 2013,

http://tecnologia.elpais.com/tecnologia/2013/01/18/actualidad/1358517550_531128.html

Emspak, Jesse, 'iPhone Flies Drone From 3,000 Miles Away', September 28th 2011, http://news.discovery.com/tech/apps/iphone-flies-drone-3000-miles-away-110928.htm

European Commission, Commission Regulation (EU) No 1141/2011 of 10 November 2011 amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:293:0022:0023:EN:PDF

European Commission, Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports COM (2010) 311 of June 15th 2010, available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0311:FIN:EN:PDF

European Commission, staff working document 'Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)', SWD (2012) 259 final, September 4th 2012, www.uasvision.com/wp-content/uploads/2012/09/EC_SWD_Euro-Strategy-RPAS_120904.pdf

European Digital Rights (EDRI), 'Police frequently use Silent SMS to locate suspects', February 1st 2012, www.edri.org/edrigram/number10.2/silent-sms-tracking-suspects

European Telecommunication Standards Institute (ETSI), DTR 101 567 V0.0.5 draft technical report (March 2012), www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_LI/2012_45_Bratislava/SA3LI12_044.doc

Fallows, James, theAtlantic.com, 'Technology Is Our Friend … Except When It Isn't' August 27th 2011, www.theatlantic.com/technology/archive/2011/08/technology-is-our-friend-except-when-it-isnt/244233/

Federal Communications Commission of the Unites States of America, 'FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps', August 5th 2005, https://w2.eff.org/Privacy/Surveillance/CALEA/FCC_voip_wiretaps.pdf

Federrath, Hannes, 'Vertrauenswürdiges Mobilitätsmanagement in Telekommunikationsnetzen', Dissertation, Technical University of Dresden, Informatics Faculty, February 1998

Femia, Will, TheMaddowBlog, 'Lawnmowers in the Dark', November 21st 2012, http://maddowblog.msnbc.com/_news/2012/11/21/15343130-lawnmowers-in-the-dark

Ferris, David, 'This Solar-Powered Drone Will Watch You All Day', August 16th 2012, www.forbes.com/sites/davidferris/2012/08/16/this-solar-powered-drone-will-watch-you-all-day/

Fidh online press release October 19th 2011, 'FIDH and LDH file a complaint concerning the responsibility of the company AMESYS in relation to acts of torture', www.fidh.org/FIDH-and-LDH-file-a-complaint

Fidh online press release January 17th 2012, 'Amesys Case: The Investigation Chamber green lights the investigative proceedings on the sale of surveillance equipment by Amesys to the Khadafi regime', www.fidh.org/Amesys-File-The-Investigation-12752

Franceschi-Bicchierai, Lorenzo, Wired.com, 'Russia Is Stockpiling Drones to Spy on Street Protests', July 25, 2012, www.wired.com/dangerroom/2012/07/russia-2/?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=Previous

Franklin, Jonathan, *The Observer*, 'Whaling: campaigners use drones in the fight against Japanese whalers', January 1st 2012, www.guardian.co.uk/environment/2012/jan/01/drones-fight-japanese-whalers

Freudiger, Julien, École Polytechnique Féderale de Lausanne, 'When Whereabouts is No Longer Thereabouts: Location Privacy in Wireless Networks' (2011)

Fried, Stephen D., CSSIP, 'Enhancing Security Through Biometric Technology', Chapter 1 in *Handbook of Information Security Management* published by Micki Krause, Harold F. Tipton, 5th edition 2004

Frye, Michelle C., Master of Arts thesis submitted to the Faculty of the Graduate School of Arts and Sciences of Georgetown University, 'The body as a password: Considerations, uses, and concerns of biometric technologies', April 27th 2001,

F-Secure Blog, '440,783 "Silent SMS" Used to Track German Suspects in 2010', December 29th 2011, https://www.f-secure.com/weblog/archives/00002294.html

Fuchs, Christian, 'Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society', The Privacy & Security Research Paper Series issue #1 July 2012, www.projectpact.eu/documents-1/%231_Privacy_and_Security_Research_Paper_Series.pdf

Gallagher, Sean, arstechnica.com, 'Big Brother on a budget: How Internet surveillance got so cheap', September 27th 2012, http://arstechnica.com/information-technology/2012/09/big-brother-meets-big-data-the-next-wave-in-net-surveillance-tech/

Galperin, Eva and Marquis-Boire, Morgan, Electronic Frontier Foundation, 'New Malware Targeting Syrian Activists Uses Blackshades Commercial Trojan', July 12, 2012, https://www.eff.org/deeplinks/2012/07/new-blackshades-malware

Gardham, Duncan, *The Telegraph*, 'Airport face scanners "cannot tell the difference between Osama bin Laden and Winona Ryder"', April 5th 2009, www.telegraph.co.uk/news/uknews/law-and-order/5110402/Airport-face-scanners-cannot-tell-the-difference-between-Osama-bin-Laden-and-Winona-Ryder.html

German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), 'Einführung in die technischen Grundlagen der biometrischen Authentisierung', https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf?__blob=publicationFile

German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), 'Grundsätzliche Funktionsweise biometrischer Verfahren', https://www.bsi.bund.de/ContentBSI/Themen/Biometrie/AllgemeineEinfuehrung/einfuehrung.html

Gibb, Alexandra, 'A Drone Field Guide', May 31st 2012, www.opencanada.org/features/the-think-tank/graphic/a-drone-field-guide/

Gill, Martin and Spriggs, Angela, Home Office Research, Development and Statistics Directorate, 'Assessing the impact of CCTV', February 2005, http://webarchive.nationalarchives.gov.uk/20110218135832/http://rds.homeoffice.gov.uk/rds/pdfs05/hors292.pdf

Gómez Mármol, Félix; Sorge, Christoph; Petrlic, Ronald; Ugus, Osman; Westhoff, Dirk; Martinez Perez, Gregorio, 'Privacy Enhanced Architecture for Smart Metering', International Journal of Information Security, vol. 12 no. 2, pp. 67-82 (2013)

Goold, Benjamin J., University of British Columbia, in 'CCTV and Human Rights', published in the 'Citizens, Cities and Video-Surveillance' paper of the European Forum for Urban Security publication of June 2010, titled 'Citizens, Cities and Video Surveillance – Towards a democratic and responsible use of CCTV', www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_publication_EN.pdf

Gorman, Siobhan; Dreazen, Yochi J.; Cole, August, 'Insurgents Hack U.S. Drones', December 17th 2009, www.online.wsj.com/article/SB126102247889095011.html#

Grabell, Michael and Salewski, Christian, 'Sweating Bullets: Body Scanners Can See Perspiration as a Potential Weapon', December 19th 2011, www.propublica.org/article/sweating-bullets-body-scanners-can-see-perspiration-as-a-potential-weapon

Greveler, Ulrich; Justus, Benjamin; Löhr, Dennis, 'Identifikation von Videoinhalten über granulare Stromverbrauchsdaten', Proceedings of Sicherheit 2012, LNI P-195, 2012, pp. 35-45 (2012)

Greveler, Ulrich; Justus, Benjamin; Löhr, Dennis: 'Forensic content detection through power consumption', ICC 2012, pp. 6759-6763 (2012)

Hansen, Marit, 'Concepts of Privacy-Enhancing Identity Management for Privacy-Enhancing Security Technologies', D 7.3 PRISE Conference Proceedings 'Towards privacy enhancing security technologies – the next steps' (2009), pp. 91-103, http://www.prise.oeaw.ac.at/docs/PRISE_D7.3_Concluding_Conference_Proceedings.pdf

Harris, Glenn, 'Southampton engineers fly the world's first "printed" aircraft', July 28th 2011, www.eurekalert.org/pub_releases/2011-07/uos-sef072811.php

Harvard School of Engineering and Applied Sciences website article 'In new mass-production technique, robotic insects spring to life', February 15th 2012, www.sciencedaily.com/releases/2012/02/120215155309.htm

Heller, Arnie, *Science & Technology Review*, issue April/May 2011, 'From Video to Knowledge', https://str.llnl.gov/AprMay11/vaidya.html

Hilty, Lorenz; Oertel, Britta; Wölk, Michaela; Pärli, Kurt, Zentrum für Technologiefolgen-Abschätzung (TA-Swiss, 'Lokalisiert und identifiziert – wie Ortungstechnologien unser Leben verändern' (2012), www.ta-swiss.ch/ortungstechnologien/

Hochstätter, Christoph H., '28C3: Hacker manipulieren Daten von intelligenten Stromzählern' (2011), www.zdnet.de/41559104/28c3-hacker-manipulieren-daten-von-intelligenten-stromzaehlern/

Hosein, Gus, Privacy International, 'Council of Europe refuses to investigate biometrics privacy', May 12th 2011, https://www.privacyinternational.org/blog/council-of-europe-refuses-to-investigate-biometrics-privacy

H Security Blog, 'Multi-platform spyware penetrates smartphones and VMs', August 22nd 2012, www.h-online.com/security/news/item/Multi-platform-spyware-penetrates-smartphones-and-VMs-1672259.html

Hull, Liz, *Mail Online*, "Drone makes first UK 'arrest' as police catch car thief hiding under bushes", February 12th 2010, http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html

Human Rights Watch, 'Losing Humanity', November 19th 2012, www.hrw.org/reports/2012/11/19/losing-humanity

Humphreys, Todd, 'How to fool a GPS', www.ted.com/talks/todd_humphreys_how_to_fool_a_gps.html

Humphreys, Todd, 'Statement on privacy issues related to the domestic use of unmanned aerial vehicles', October 25th 2012, field forum on privacy issues related to the domestic use of drones, a forum sanctioned by the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security

Humphreys, Todd, The Cockrell School of Engineering/The University of Texas at Austin, TEDx video and script, 'The GPS Dot and Its Discontents', March 8th 2012, www.engr.utexas.edu/features/7233-humphreysgps

Hustinx, Peter, European Data Protection Supervisor, Opinion of February 1st 2011 on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development – Turbine (TrUsted Revocable Biometric IdeNtitiEs), www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf

Hustinx, Peter, European Data Protection Supervisor, 'Video surveillance guidelines', March 17th 2010, www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

International Association for Identification (IAI), website information 'Biometrics Information Systems', www.theiai.org/disciplines/biometrics/index.php

International Telecommunication Union (ITU), 'ITU-T Y.2770, Requirements for Deep Packet Inspection in Next Generation Networks', www.itu.int/rec/T-REC-Y.2770-201211-P

Introna, Lucas D., Lancaster University, UK; Centre for the Study of Technology and Organization and Nissenbaum, Helen, New York University; Department of Media, Culture, and Communication, 'Facial Recognition Technology – A Survey of Policy and Implementation Issues', report created for the Center for Catastrophe Preparedness & Response, New York University, July 22nd 2009; Computer Science, and the Information Law Institute, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1437730

ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV), definition no. 37.05.10 and definition no. 37.05.12

Jawurek, Marek; Kerschbaum, Florian; Danezis, George, 'Privacy Technologies for Smart Grids – A Survey of Options', Microsoft Technical Report MSR-TR-2012-119, November 2012, https://research.microsoft.com/apps/pubs/?id=178055

Karg, Moritz, 'Biometrische Verfahren zur Gesichtserkennung und Datenschutz in Sozialen Netzwerken', issue 7/2012 Humbold Forum Recht, p. 120 ff., www.humboldt-forum-recht.de/media/Druckansicht/pdf/2012-07.pdf

Kaye, Ken, *Los Angeles Times*, 'Tiny aircraft could improve hurricane forecasts', September 30th 2011, http://articles.latimes.com/2011/sep/30/nation/la-na-hurricane-drone-20111001

Köpsell, Stefan; Wendolsky, Rolf; Federrath, Hannes, 'Revocable Anonymity', Proceedings of Emerging Trends in Information and Communication Security: International Conference, ETRICS 2006, LNCS 3995, pp. 206-220 (2006)

Köpsell, Stefan, 'Entwicklung und Betrieb eines Anonymisierungsdienstes', Dissertation, Technical University of Dresden, Informatics Faculty, March 2010

Krebs, Brian, 'FBI: Smart Meter Hacks Likely to Spread' (2012), http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

Królikowski, Agata, Humboldt-University of Berlin, 'Due To Legal Issues – Packet Inspection', diploma thesis, March 24th 2012, http://waste.informatik.hu-berlin.de/agata/docs/due_to_legal_issues_pi_v_1_3.pdf

Kropatsch, Walter and Sablatnig, Robert, Pattern Recognition and Image Processing Group at the Institute of Computer-aided Automation, Computer Science Department of the Vienna University of Technology, 'Biometrics'

Kursawe, Klaus; Danezis, George; Kohlweiss, Markulf, 'Privacy-Friendly Aggregation for the Smart-Grid', Privacy Enhancing Technologies – 11th International Symposium, PETS 2011, pp. 175-191 (2011)

Kushan, Melih Cemal, Faculty of Engineering and Architecture, Eskisehir Osmangazi University, Eskisehir in Turkey, 'The relationship between the UAV fleet of European countries and their geopoliticial position', publication for the International Conference of Scientific Paper AFASES 2012, Brasov, 24–26 May 2012, http://connection.ebscohost.com/c/articles/82405348/relationship-between-uav-fleet-european-countries-their-geopolitical-position

Laja, Sade, Guardian Professional Networks, 'Councils spend £515m in four years on CCTV', February 21st 2012, www.guardian.co.uk/government-computing-network/2012/feb/21/cctv-councils-big-brother-watch?INTCMP=SRCH

Leyden, John, 'Iran spy drone GPS hijack boasts: Rubbish, say experts', white paper of December 21st 2011, www.theregister.co.uk/2011/12/21/spy_drone_hijack_gps_spoofing_implausible/

Lichtblau, Eric, *The New York Times*, 'Wireless Firms Are Flooded by Requests to Aid Surveillance', July 8th 2012, www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?_r=2&ref=surveillanceofcitizensbygovernment

Liebelson, Dana, 'Google-Funded Drones To Hunt Rhino Poachers', December 5th 2012, www.motherjones.com/blue-marble/2012/12/rhino-poacher-meet-drone-funded-google

Lischka, Konrad, *Spiegel Online*, 'Marktforschung per Gesichtsanalyse: Schau mich an – und ich weiß, wer du bist', November 17th 2011, www.spiegel.de/netzwelt/netzpolitik/marktforschung-per-gesichtsanalyse-schau-mich-an-und-ich-weiss-wer-du-bist-a-797683.html

Lißmann, Carsten, *Zeit Online*, 'Die unsichtbaren Ermittler' (translated: 'The invisible investigators'), January 1st 2008, www.zeit.de/online/2008/03/unbemannte-drohnen-hooligans-sachsen

Lockheed Martin, 'Laser Powers Lockheed Martin's Stalker UAS for 48 Hours', July 11th 2012, www.lockheedmartin.com/us/news/press-releases/2012/july/120711ae_stalker-UAS.html

Lynch, Jennifer, Electronic Frontier Foundation, 'FBI's Facial Recognition is Coming to a State Near You', August 2nd 2012, https://www.eff.org/deeplinks/2012/07/fbis_facial_recognition_coming_state_near_you

Lynch, Jennifer, Electronic Frontier Foundation, 'Newly Released Drone Records Reveal Extensive Military Flights in US', December 5th 2012, https://www.eff.org/deeplinks/2012/12/newly-released-drone-records-reveal-extensive-military-flights-us

Maass, Peter and Rajagopalan, Meghda, *The New York Times* Sunday Review, 'That's Not My Phone. That's My Tracker', July 13th 2012, https://www.nytimes.com/2012/07/15/Sunday-review/thats-not-my-phone-its-my-tracker.html?_r=3&src=rechp

Manyika, James; Chui, Michael; Brown, Brad; Bughin, Jacques; Dobbs, Richard; Roxburgh, Charles; Hung Byers, Angela, McKinsey Global Institute Report, 'Big data: The next frontier for innovation, competition, and productivity', May 2011, www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation

Marquis-Boire, Morgan and Marczak, Bill, 'The SmartPhone Who Loved Me: FinFisher Goes Mobile?', The Citizen Lab at the University of Toronto, Research Brief Number 11, August 2012, https://citizenlab.org/wp-content/uploads/2012/08/11-2012-thesmartphonewholovedme.pdf

Martin, Hugo, *Los Angeles Times*, 'Are TSA officers laughing at you? Agency says no', January 6th 2013, www.latimes.com/business/la-fi-mo-tsa-officers-laughing-20130103,0,1200411.story

Mathieson, S.A. and Evans, Rob, *The Guardian*, 'Roadside cameras suffer from large gaps in coverage, police admit', August 27th 2012, www.guardian.co.uk/uk/2012/aug/27/police-number-plate-cameras-network-patchy

Mazzetti, Mark, *The New York Times*, 'The Drone Zone', July 6th 2012, www.nytimes.com/2012/07/08/magazine/the-drone-zone.html?pagewanted=all&_r=0

McCaney, Kevin, 'Army's "sense and avoid" radar will let drones fly in domestic airspace', July 10th 2012, http://gcn.com/articles/2012/07/10/army-sense-avoid-radar-gbsaa-drone-technology.aspx

McNeal, Greg, Forbes.com, 'London Olympics Security Focuses on Deterrence: Use of Drones, Electric Fences, Missiles and More', June 23rd 2012, www.forbes.com/sites/gregorymcneal/2012/07/23/london-olympics-security-focuses-on-deterrence-use-of-drones-electric-fences-missiles-and-more/

Meister, Andre, Netzpolitik.org, 'Deep Packet Inspection: Der Unterschied zwischen Internet in Diktaturen und Deutschland ist nur eine Konfigurationsdatei', November 8th 2012, https://netzpolitik.org/2012/deep-packet-inspection-der-unterschied-zwischen-internet-in-diktaturen-und-deutschland-ist-nur-eine-konfigurationsdatei/#more-38469

Meister, Andre, Netzpolitik.org, 'Funkzellenabfragen bei NSU-Ermittlungen: 20 Millionen Verbindungsdaten, 14,000 Namen und Adressen, 0 Täter', October 19th 2012, https://netzpolitik.org/2012/funkzellenabfragen-bei-nsu-ermittlungen-12-millionen-verbindungsdaten-14-000-namen-und-adressen-0-verdachtige/

Meléndez-Juarbe, Hiram A., University of Puerto Rico Law School, 'Intermediaries and Freedom of Expression', essay translated by University students Edgardo Canales and Marini Rodriguez, www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/04-Intermediaries_Freedom_of_Expression_Hiram_Melendez_Juarbe.pdf

Menn, Joseph, 'Social networks scan for sexual predators, with uneven results', July 12th 2012, www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712

Mert, Wilma; Suschek-Berger, Jürgen; Čas, Johann et al., 'Final Report – Smart New World?' (2012)

Michaels, Jim, *USA TODAY*, 'Military turns to ESPN to help analyze drone footage', December 19th 2012, www.usatoday.com/story/news/nation/2012/12/19/drone-video/1770337/

MIKE2.0, the open source standard for Information Management, www.mike2.openmethodology.org/wiki/Big_Data_Definition

Mochalski, Klaus and Schulze, Hendrik, 'Deep Packet Inspection – Technology, Applications & Net Neutrality', white paper (2009) for the company ipoque www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf

Moss, David, *The Register*, 'Collar the lot of us! The biometric delusion – Optimism beats evidence in the drive to fingerprint the world', August 14th 2009, www.theregister.co.uk/2009/08/14/biometric_id_delusion/

Müller, Klaus J., 'Gewinnung von Verhaltensprofilen am intelligenten Stromzähler' article published in DuD – *Datenschutz und Datensicherheit*, vol. 6/2010; www.secorvo.de/publikationen/verhaltensprofile-smart-meter-mueller-2010.pdf

Mueller, Milton, Syracuse University School of Information Studies, 'DPI Technology from the standpoint of Internet governance studies: An introduction', October 21st 2011, http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf

Mulliner, Collin, Heise Security, 'Scan in Mobilfunknetzen fördert tausende ungeschützte Geräte zu Tage', July 27th 2012, www.heise.de/newsticker/meldung/Scan-in-Mobilfunknetzen-foerdert-tausende-ungeschuetzte-Geraete-zu-Tage-1653619.html

Nakashima, Ellen and Whitlock, Craig, *The Washington Post*, 'With Air Force's Gorgon Drone "we can see everything"', January 2nd 2011, www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html

National Institute of Standards and Technology (NIST), special publication 800-77, 'Guide to Ipsec VPNs', http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

National Institute of Standards and Technology (NIST), The Smart Grid Interoperability Panel – Cyber Security Working Group, 'Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid' (2010), http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

Newcomb, Doug, Wired.com, 'How Big Data Will Ease Your Commute', November 21st 2012,

www.wired.com/autopia/2012/11/big-data-commute/

Nighswander, Tyler; Brumley, Robert; Ledvina, Brent; Brumley, David; Diamond, Jonathan, 'GPS Software Attacks', CS'12 paper October 2012, http://users.ece.cmu.edu/~dbrumley/courses/18487-f12/readings/Nov28_GPS.pdf

Norris, Clive; McCahill, Mike; Wood, David, 'The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space', published in the *Surveillance & Society*, vol. 2, no. 2/3 (2004), titled 'The Politics of CCTV in Europe and Beyond'

Ohaneme, Cletus O.; Eke, James; Azubogu, Augustine C.O.; Ifeagwu, Emmanuel N.; and Ohaneme, Louisa C., 'Design and Implementation of an IP-Based Security Surveillance System', *IJCSI International Journal of Computer Science Issues*, vol. 9, issue 5, no 1, September 2012, p. 393, accessible at: www.ijcsi.org/papers/IJCSI-9-5-1-391-400.pdf

Ohm, Paul, *Harvard Business Review* Blog Network, 'Don't Build a Database of Ruin', August 23rd 2012, www.blogs.hbr.org/cs/2012/08/dont_build_a_database_of_ruin.html

Otten, Bettina, '3D Gesichtserkennung – Merkmalsdetektion in 3D-Scans und merkmalsbasierter Vergleich von Gesichtern', dissertation at the University Koblenz Landau March 2006, http://de.pdfsb.com/readonline/593142446541462b586e42314433786a56413d3d-4567740

Petri, Thomas, Bavarian Data Protection Commissioner in Germany, 'Prüfbericht Quellen-TKÜ', July 30th 2012, www.datenschutz-bayern.de/0/bericht-qtkue.pdf

Phillips, P. Jonathon; Grother, Patrick; Micheals, Ross; Blackburn, Duane M.; Tabassi, Elham; and Bone, Mike, 'Face Recognition Vendor Test 2002', DARPA et al., Arlington 2003

Pickles, Nick, Big Brother Watch article published May 14, 2012, 'London MET police spends £4m a year watching CCTV', www.bigbrotherwatch.org.uk/home/2012/05/met-cctv-4m-spendin.html

Pickles, Nick, 'Eyes on the Olympics', July 25th 2012, www.bigbrotherwatch.org.uk/home/2012/07/eyes-on-the-olympics.html

Poggioli, Sylvia, NPR News, 'With A Database, Germany Tracks Rise Of Neo-Nazis', October 11th 2012, www.npr.org/2012/10/11/162663914/with-a-database-germany-tracks-rise-of-neo-nazis

Posel, Susanne, 'The Insects Are Watching: The Future of Government Surveillance Technology', http://amresolution.com/2012/06/18/the-insects-are-watching-the-future-of-government-surveillance-technology/

PRISE project (Privacy & Security), D2.2 (Overview of Security technologies), February 2006, revised April 2007, www.prise.oeaw.ac.at/publications.htm

Privacy International, 'CCTV Frequently Asked Questions', June 21th 1997, https://www.privacyinternational.org/blog/cctv-frequently-asked-questions

Privacy International, 'Draft Communications Bill reveals Home Office's mass surveillance plans going ahead – but government remains tongue-tied about how technology will actually work', June 15th 2012, https://www.privacyinternational.org/press-releases/draft-communications-bill-reveals-home-offices-mass-surveillance-plans-going-ahead

Prokoski, Francine, 'History, Current Status, and Future of Infrared Identification', published in year 2000 in IEEE Computer Society, Computer Vision beyond the Visible Spectrum: Methods and Applications, www.marathon.cse.usf.edu/~sarkar/biometrics/papers/IRSummary.pdf

Protalinski, Emil, TheNextWeb, 'The FBI pours $1 billion into facial recognition technology project, going nationwide in 2014', http://thenextweb.com/insider/2012/09/07/the-fbi-pours-1-billion-facial-recognition-technology-project-going-nationwide-2014/

Rattani, Ajita, 'Adaptive Biometric System based on Template Update Procedures', Ph.D. thesis at the University of Cagliari, Department of Electrical and Electronic Engineering (2010)

Reuters article, 'Police drones to be equipped with non-lethal weapons?', March 14th 2012, http://rt.com/usa/news/drone-surveillance-montgomery-weapon-507/

Rial, Alfredo and Danezis, George, 'Privacy-Preserving Smart Metering', Proceedings of the 2011 ACM Workshop on Privacy in the Electronic Society, WPES 2011, pp. 49-60 (2011)

Robertson, Adi, theverge.com, 'Military-backed surveillance prototype can read people's actions on video', October 28th 2012, www.theverge.com/2012/10/28/3567048/carnegie-mellon-video-surveillance-action-recognition

Rooney, Ben, *The Wall Street Journal*, 'Airship Plan to Put Cameras in the Sky', November 19th 2012, http://blogs.wsj.com/tech-europe/2012/11/19/croatian-airship-plan-to-put-cameras-in-the-sky/

Roth, Jörg, University of Hagen, in 'Location-Based Services' by Jochen Schiller & Agnés Voisard (2004)

Rouse, Margaret, SearchMobileComputing, definition entries for the terms 'Geolocation', http://searchmobilecomputing.techtarget.com/definition/geolocation, 'Location-based service (LBS)', www.searchnetworking.techtarget.com/definition/location-based-service-LBS, 'Biometric Terms: Glossary', http://whatis.techtarget.com/reference/Biometric-Terms-Glossary

Sander, Alexander, Netzpolitik.org, 'INDECT ist nur ein Symptom – EU-Forschung braucht effektive Kontrolle!' October 9th 2012, https://netzpolitik.org/2012/indect-ist-nur-ein-sympton-eu-forschung-braucht-effektive-kontrolle/

Schaar, Peter, Federal Commissioner for Data Protection and Freedom of Information in Germany, 'Biometrics and chip identity cards in everyday working life', www.bfdi.bund.de/EN/Topics/labour/Artikel/BiometricsChipIdentities.html

Schäfer, Christian, 'Effiziente Architekturen und Technologien zur Realisierung von Smart Metering im Bereich der Nahkommunikation', GRIN Verlag (2010)

Schoen, Seth, Electronic Frontier Foundation, 'Legal Struggles Over Interception Rules in the United States', https://www.eff.org/pages/legal-struggles-over-interception-rules-united-states

Schroyer, Matthew, DroneJournalism.org, 'A drone crash in a populated area, and a friendly reminder on drone safety', October 27th 2012, www.dronejournalism.org/blog/adronecrashinapopulatedareaandafriendlyreminderondronesafety

Security Middle East Magazine, issue 65 March/April 2012, titled 'Improving situational awareness', www.securitymiddleeastmagazine.com/features/view/32

Shachtman, Noah, Wired.com, 'Exclusive: Computer Virus Hits U.S. Drone Fleet', June 10th 2011, www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

Shachtman, Noah and Axe, David for Wired.com, 'Most U.S. Drones Openly Broadcast Secret Video Feeds', October 29th 2012, www.wired.com/dangerroom/2012/10/hack-proof-drone/

Siddiqui, Salman, 'Celebrating Paksat-1R: Pakistani drones – a dream or reality?', August 6th 2012, http://tribune.com.pk/story/418118/celebrating-paksat-1r-pakistani-drones-a-dream-or-reality/

Silver, Vernon, Bloomberg.com, 'Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma', July 25, 2012, www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html

Singh, Abhishek and Kumar, Saurabh, Department of Computer Science and Engineering National Institute of Technology Rourkela in India, "Face Recognition using PCA and Eigen face approach", Btech thesis (2012), http://ethesis.nitrkl.ac.in/3814/

Smith, Matt, CNN.com, 'Flying drone peers into Japan's damaged reactors', April 10th 2011, http://articles.cnn.com/2011-04-10/world/japan.nuclear.reactors_1_radioactive-water-tokyo-electric-power-reactors?_s=PM:WORLD

Sonne, Paul and Coker, Margaret, *The Wall Street Journal Online*, 'Firms aided Libyan spies – First Look Inside Security Unit Shows How Citizens Were Tracked', August 30th 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html#

Soyez, Fabien, QWNI News, 'Getting the Message? Police Track Phones with Silent SMS', January 27th 2012, http://owni.eu/2012/01/27/silent-sms-germany-france-surveillance-deveryware/

Spanish Data Protection Agency of Surveillance, Instruction 1/2006

Squires, Peter, University of Brighton, 'Evaluating CCTV: Lessons from a Surveillance Culture', published on pp. 39 ff. in the 'Citizens, Cities and Video-Surveillance' paper of the European Forum for Urban Security publication of June 2010, titled 'Citizens, Cities and Video Surveillance – Towards a democratic and responsible use of CCTV'

Stanford Law School – International Human Rights and Conflict Resolution Clinic, and Global Justice Clinic at NYU School of Law, 'Living under drones: Death, injury, and trauma to civilians from US drone practices in Pakistan' (2012), http://livingunderdrones.org/

Stedmon, Alex, 'The camera never lies, or does it? The dangers of taking CCTV surveillance at face value and the importance of human factors', *Surveillance & Society*, vol. 9, no. 3 (2012) 'Urban Surveillance', http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/4192/4194

Strobel, Daehyun, Ruhr-University Bochum, Chair for Communication Security, 'IMSI Catcher', July 13th 2007

Suarez, Daniel interviewed by Rieger, Frank, in *Frankfurter Allgemeine* about his recently published book 'Kill Decision', September 24th 2012, www.faz.net/aktuell/feuilleton/debatten/digitales-denken/frank-rieger-interviews-daniel-suarez-swarming-killing-machines-11901656.html

Talbot, David, *MIT Technology Review*, 'A Phone That Knows Where You're Going – An algorithm can better predict your future movements by getting a little help from your friends', July 9th 2012, www.technologyreview.com/news/428441/a-phone-that-knows-where-youre-going/

David Talbot, *MIT Technology Review*, 'Wiping Away Your Siri 'Fingerprint'', June 28th 2012, http://www.technologyreview.com/news/428053/wiping-away-your-siri-fingerprint/

Tauber, Andre, *Die Welt*, 'Die Superdrohne ist ein riesiger Datenstaubsauger' (translated: 'The super drone is a giant data hoover'), available in German at: www.welt.de/wirtschaft/article112713975/Die-Superdrohne-ist-ein-riesiger-Datenstaubsauger.html

Taylor, Nick, *Surveillance & Society*, vol. 1, no. 1 (2002) 'State Surveillance and the Right to Privacy', www.surveillance-and-society.org/articles1/statesurv.pdf

TELETRUST Deutschland e.V., Arbeitsgruppe Biometrie, ' Datenschutz in der Biometrie', white paper, Redaktion: H. Biermann, M. Bromba, C. Busch, G. Hornung, M. Meints, G. Quiring-Kock, version of March 11th 2008, www.teletrust.de/publikationen/whitepapers/

The Associated Press on CBS News, 'TSA quietly removing some full body scanners', October 25th 2012, www.cbsnews.com/8301-201_162-57540714/tsa-quietly-removing-some-full-body-scanners/

The National IT and Telecom Agency, Copenhagen, Denmark: New Digital Security Models – Discussion Paper, February 2011

TheOpenNet Initiative, 'Global Internet filtering in 2012 at a glance', April 3rd 2012, http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance and 'About filtering', http://opennet.net/about-filtering

Thomson, Wendy, 'Ignore the man behind the curtain', February 29th 2012, www.tsanewsblog.com/1750/news/ignore-the-man-behind-the-curtain/

Timberg, Craig and Nakashima, Ellen, *The Washington Post*, 'Skype makes chats and user data more available to police', July 26th 2012, www.washingtonpost.com/business/economy/skype-makes-chats-and-user-data-more-available-to-police/2012/07/25/gJQAobl39W_story.html

Timm, Trevor, Electronic Frontier Foundation, 'Law Enforcement Agencies Demanded Cell Phone User Info Far More Than 1.3 Million Times Last Year', July 9th 2012, https://www.eff.org/deeplinks/2012/07/law-enforcement-agencies-demanded-cell-phone-user-info-much-more-13-million-times

Tirone, Jonathan, Bloomberg.com, 'Airport Body Scanning Raises Radiation Exposure, Committee Says', February 5th 2010, www.bloomberg.com/apps/news?pid=newsarchive&sid=aoG.YbbvnkzU&pos=11

TURBINE project (TrUsted Revocable Biometric IdeNtitiEs), public deliverable R2.3 'Practical Guidelines for the privacy friendly processing of biometric data for identity verification', www.turbine-project.eu

Ungerleider, Neal, Fast Company web blog, 'Mass Transit Cameras Spot Bad Guys, No Human Judgment Required', June 1st, 2012, www.fastcompany.com/1839052/big-brother-is-coding-you

UK Communications-Electronics Security Group, website information 'Privacy issues and biometrics', www.cesg.gov.uk/policyguidance/biometrics/Pages/MS06-Privacy-Issues.aspx

United States Court of Appeals for the District of Columbia Circuit, ruling No. 08-3030 issued August 6th 2010

University of Pennsylvania, General Robotics, Automation, Sensing and Perception (GRASP) Laboratory, www.youtube.com/watch?feature=player_embedded&v=YQIMGV5vtd4

U.S. Air Force fact sheet for the MQ-9 Reaper drone, www.af.mil/information/factsheets/factsheet.asp?fsID=6405

U.S. Department of Defense, 331 Joint publications 1-02, Dictionary of military and associated terms (2010), amended July 15, 2012

U.S. Federal Trade Commission, 'Facing Facts – Best Practices for Common Uses of Facial Recognition Technologies', October 2012, http://ftc.gov/os/2012/10/121022facialtechrpt.pdf

U.S. Government Accountability Office (GAO) report on the proliferation of UAVs of July 2012

vieuxrenard, ijure.org, 'Skype likely to provide means of VoIP interception – eavesdropping by "state trojans" disproportionate', January 15th 2012, http://ijure.org/wp/archives/833

Vumii Inc., 'Continuous Wave Laser Illumination: The Clear Choice over Thermal Imaging for Long-Range, High-Magnification Night Vision Perimeter Protection', September 2008

Wagner, Ben, Ludwig-Maximilians-Universität München and Universität Leiden, 'Deep Packet Inspection and Internet Censorship: International Convergence on an "Integrated Technology of Control"', paper for Global Voices Advocacy (2008), http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf

Wahlbrink, Joachim, Data Protection Commissioner of Niedersachsen, Germany, 'Funk-Überwachungskameras – ein häufig unterschätztes Problem', www.lfd.niedersachsen.de/portal/live.php?navigation_id=13098&article_id=56224&_psmand=48

Warne, Gary C., 'The Predator's Ancestors – UAVs in The Great War', July 25th 2012, http://warnepieces.blogspot.de/2012/07/the-predators-ancestors-uavs-in-great.html

Warwick, Graham, Ares Defense Technology Blog, 'Hovering Near You – IARPA's Quiet UAV', July 18th 2012, www.aviationweek.com/Blogs.aspx?plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3a27bcb5c2-5216-4ed5-b53d-1e6f0fc2c0a5

Watson, Paul Joseph, Prisonplanet.com, 'TSA To Test Body Scanner Operators For Radiation Exposure', January 16th 2012, www.infowars.com/tsa-to-test-body-scanner-operators-for-radiation-exposure/

Watson, Steve, Prisonplanet.com, 'More New Documents Show TSA Intends To Deploy Body Scanners At Rail, Bus, Ferry Terminals', September 7th 2012, www.prisonplanet.com/more-new-documents-show-tsa-intends-to-deploy-body-scanners-at-rail-bus-ferry-terminals.html

Weichert, Thilo, 'Drohnen und Datenschutz – Bedrohungspotenzial und Gesetzgebungsbedarf bei der Beobachtung von oben' *Zeitschrift für Datenschutz* (ZD), issue 11/2012

Weintraub, Karen, *The New York Times*, 'But How Do You Really Feel? Someday the Computer May Know', October 15th 2012, https://www.nytimes.com/2012/10/16/science/affective-programming-grows-in-effort-to-read-faces.html?_r=2&

Wikileaks Spyfiles, document #289, 'Remote Monitoring & Infection Solutions: FINSPY', http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf

ZEIT Online, 'Mail-Überwachung durch Geheimdienste deutlich gestiegen', February 25th, 2012, www.zeit.de/digital/datenschutz/2012-02/geheimdienst-ueberwachung-email

Zenko, Micah and Fellow, Douglas Dillon, '9/11 Lessons: Unconventional Warfare', article published August 26th 2011 for the Council on Foreign Relations website, www.cfr.org/united-states/911-lessons-unconventional-warfare/p25661

Zetter, Kim, 'DIY Spy Drone Sniffs Wi-Fi, Intercepts Phone Calls', August 4th 2011, http://nonviolentconflict.wordpress.com/2012/03/09/diy-spy-drone-sniffs-wi-fi-intercepts-phone-calls/

Zhao, Yisu, Ph.D. thesis submitted to the Faculty of Graduate and Postdoctoral Studies, Ottawa-Carleton Institute for Computer Science, 'Human Emotion Recognition from Body Language of the Head using Soft Computing Techniques', www.ruor.uottawa.ca/en/bitstream/handle/10393/23468/Zhao_Yisu_2012_thesis.pdf?sequence=1

Zhou, Xuebing, thesis submitted to the Technische Universität Darmstadt, 'Privacy and Security Assessment of Biometric Template Protection' (2012), http://tuprints.ulb.tu-darmstadt.de/2885/

Zucchino, David, *Los Angeles Times*, 'War zone drone crashes add up', July 6th 2010, http://articles.latimes.com/2010/jul/06/world/la-fg-drone-crashes-20100706

5 List of Figures

6 List of Tables