CYBERLAWS 2012

The Third International Conference on Technical and Legal Aspects of the e-Society

ISBN: 978-1-61208-182-3

January 30- February 4, 2012

Valencia, Spain

CYBERLAWS 2012 Editors

Lasse Berntzen, Vestfold University College - Tønsberg, Norway

Claus-Peter Rückemann, Leibniz Universität Hannover / Westfälische Wilhelms-Universität Münster / North-German Supercomputing Alliance (HLRN), Germany

CYBERLAWS 2012

Forward

The Third International Conference on Technical and Legal Aspects of the e-Society (CYBERLAWS 2012), held in Valencia, Spain, on January 30th – February 4th, 2012, followed the multiplications of the cybercrime acts concerning privacy and anonymity in the information society.

In accordance with the principle of freedom of expression and the right to privacy, the use of anonymity is legal. Users can access data and browse anonymously so that their personal details cannot be recorded and used without their knowledge by any other entity, including another user. As there are situations were content/information providers might wish to remain anonymous for legitimate purposes, they should not be required to justify anonymous use. The dangerous side of the legal anonymity is the shadow for illegal, damaging, and not easily to sue individuals and actions. Corporate and individual hassle, corporate and individual frauds, threats, and impersonations are only a few of these actions. While privacy, anonymity and freedom of speech are achieved rights, there is a vacuum on education, punishments, and laws that can be easily applied at the same velocity with which a cybercrime propagates. Applying the Civil Court legislation is tedious and naturally, too late to timely repair the damage and prevent its quick propagation. There is a need for special laws to either prevent or quickly reprimand. In this case, the identity must be legally and undoubtedly validated. In this case, the identity must be legally and undoubtedly validated. There is a need of internationally adopted guidelines to be applied by victims. There is a need for harmonization between national laws for a new era of eDemocracy.

CYBERLAWS 2012 provided a forum where researchers, government representatives, international bodies, law enforcement organisms and special groups were able to present recent lessons learned, use cases, and set the priorities on problems and directions related to the anonymity, privacy, identity, and laws that should or are governing their legal use.

The event was very competitive in its selection process and very well perceived by the international scientific and industrial communities. As such, it is attracting excellent contributions and active participation from all over the world. We were very pleased to receive a large amount of top quality contributions.

The accepted papers covered topics related to e-Government, e-Democracy, Privacy, and e-Fraud. We believe that the CYBERLAWS 2012 contributions offered a panel of solutions to key problems in all areas concerning privacy and anonymity in the information society.

We take here the opportunity to warmly thank all the members of the CYBERLAWS 2012 technical program committee as well as the numerous reviewers. The creation of such focused and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and efforts to contribute to the CYBERLAWS 2012. We truly believe that thanks to all these efforts, the final conference program consists of top quality contributions.

This event could also not have been a reality without the support of many individuals, organizations and sponsors. In addition, we also gratefully thank the members of the CYBERLAWS 2012 organizing committee for their help in handling the logistics and for their work that is making this professional meeting a success.

We hope the CYBERLAWS 2012 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress on the topics of the conference.

We also hope the attendees enjoyed the beautiful surroundings of Valencia, Spain.

CYBERLAWS 2012 Chairs

Lasse Berntzen, Vestfold University College - Tønsberg, Norway
Adolfo Villafiorita, Fondazione Bruno Kessler/ University of Trento, Italy
Claus-Peter Rückemann, Leibniz Universität Hannover / Westfälische Wilhelms-Universität Münster / North-German Supercomputing Alliance (HLRN), Germany
Glenn S. Dardick, Longwood University, USA / Edith Cowan University, Australia

CYBERLAWS 2012

Committee

CYBERLAWS 2012 Advisory Committee

Lasse Berntzen, Vestfold University College - Tønsberg, Norway
Adolfo Villafiorita, Fondazione Bruno Kessler**/** University of Trento, Italy
Claus-Peter Rückemann, Leibniz Universität Hannover / Westfälische Wilhelms-Universität Münster / North-German Supercomputing Alliance (HLRN), Germany
Glenn S. Dardick, Longwood University, USA / Edith Cowan University, Australia

CYBERLAWS 2012 Technical Program Committee

Jemal Abawajy, Deakin University, Australia
Habtamu Abie, Norwegian Computing Center/Norsk Regnesentral, Norway
Evgenia Alexandropoulou, University of Macedonia - Thessaloniki, Greece
Rabih Bashroush, University of East London, UK
Ilija Basicevic, University of Novi Sad, Serbia
Farid Enrique Ben Amor, Coro Center for Civic Leadership - Southern California, USA
Salima Benbernou, Université Paris Descartes, France
Lasse Berntzen, Vestfold University College - Tønsberg, Norway
Carlo Blundo, Università di Salerno, Italy
Erik Buchmann, Karlsruhe Institute of Technology (KIT), Germany
Christian Callegari, University of Pisa, Italy
Sudip Chakraborty, Valdosta State University, USA
Clare Chambers, UWE Bristol Law School, UK
Kim-Kwang Raymond Choo, University of South Australia and Australian National University, Australia
Frédéric Cuppens, IT TELECOM Bretagne, France
Nora Cuppens-Boulahia, Telecom Bretagne, France
Kevin Curran, University of Ulster, UK
Glenn S. Dardick, Longwood University, USA / Edith Cowan University, Australia
Jana Dittmann, Otto-von-Guericke University Magdeburg, Germany
Noella Edelmann, Centre for E-Government, Danube University Krems, Austria
El-Sayed El-Alfy, King Fahd University of Petroleum and Minerals, Saudi Arabia
Benjamin Fabian, Humboldt-Universität zu Berlin, Germany
Steven Furnell, University of Plymouth, UK
Matjaz Gams, Jozef Stefan Institute-Ljubljana, Slovenia
Christos K. Georgiadis, University of Macedonia - Thessaloniki, Greece
Wasif Gilani, SAP Research Belfast, United Kingdom
Hidehito Gomi, Yahoo! Japan Research, Japan
Huong Ha, University of Newcastle, Singapore
Ali Hessami, University of East London, UK
Rajesh Ingle, PICT, Pune, India
Georgios Kambourakis, University of the Aegean - Samos, Greece

Copyright Information

Table of Contents

Indian Approach to Privacy in Cyberspace

M. Tariq Banday
Department of Electronics & Inst. Technology
University of Kashmir
Srinagar, India
e-mail: sgrmtb@yahoo.com

Farooq Ahmad Mir
Department of Law
University of Kashmir
Srinagar, India
e-mail: far_lwtr@rediffmail.com

Abstract—**Privacy as a right has genesis in the technology of printing and photography. This technology was viewed as impinging confidentiality of individual. Privacy right has been expanded over the years to enfold its other aspects and has been made actionable against an individual under law of Torts and redress-able against State under Constitutional Law for violating autonomy of an individual. Digital Technology has privacy issues. These issues cannot be addressed by applying traditional principles. Furthermore, Information Technology Act (IT Act) in India has been amended in the year 2008 which has given enormous powers to the Centre and State Governments to invade privacy. This paper makes an attempt to raise privacy issues pertinent to cyberspace, examines Indian judicial approach to constitutional right to privacy and evaluates technological approach to privacy.**

Keywords—Privacy; Interception; Monitoring; Privacy & Security; IT ACT 2008; Judicial Approach to Privacy

I. Privacy Issues in Cyberspace

Development of privacy jurisprudence is intimately associated with technological developments much before Internet came on the horizon. Its seeds were sown at the end of the nineteenth century, following the publication of Warren and Brandies article, the right to privacy [1]. This article was prompted by the technological innovations of print media (newspapers) and the portable camera (photographs) which were thought to have potential to invade personal privacy. J. Thomas Cooly in a celebrated case of *Olmstead v. United State*[1] crystalized this doctrine by declaring that every individual has a right to be let alone. Invasion of privacy means an unjustified exploitation of one's personality or intrusion into one's personal activity, actionable under tort law and sometimes under constitutional law. Initially this right was confined to what later became its essential but not exclusive component, the right to protect the confidentiality of one's private sphere against public or private interference. Soon this right was expanded to en-cover four distinct torts that may possibly arise in case of breach of privacy a) intrusion upon a person's solitude or seclusion or into his affairs, b) public disclosure of embarrassing facts of a person's private life, c) publicity which places an individual in false light in public eyes, and d) appropriation to a person's advantage of another's name or likeness [2].

The concept and the right of privacy have undergone a significant evolution, due to the Socio-economic developments and, much more, due to the introduction of the information Communications Technologies (ICT) into daily life [3]. Equally the amount of data collected by cameras and biometric systems through the use of automated devices and their intelligent use in order to provide personalized services, clearly, gives rise to privacy problems [4].

Digital technology has changed form as well as the nature of the privacy right. In recent years, the World Wide Web, particularly Web 2.0, has raised challenges for privacy, as it fuses together voices, text, pictures, recording and retrieval technologies, and a larger capacity for the incidental gathering of details of people's private lives [5]. It involves more voices than previous Internet technologies. Blogs, wikis, online social networks, and massively multiplayer online games allow more people to communicate and interact more than ever before, about their own self or about their surroundings. This raises a plethora of privacy concerns differing in content and ambit from that which was traditionally known. Earlier Internet privacy concerns related predominantly to the aggregation of personal information to create large-scale, text-based digital dossiers about individuals [6].

Interactive Web 2.0 technology has led to an increasing tendency for people to publish texts, photographs, videos, locations, tags and preferences online, thereby placing a good deal of private life on record [7]. With more voices online, there is a wider scope for privacy invasion. With more recording technologies readily at hand such as cell phone cameras and text messaging services like Twitter—there is a wider scope for incidental gathering of details of people's private lives that can be uploaded and disseminated globally at the mouse click.

These developments have blurred the boundaries between the public and private spheres or at least are becoming more difficult to discern. Thus, any privacy laws premised on conceptions of a "reasonable expectation of privacy" are becoming more difficult to apply [8]. Facebook founder Mark Zuckerberg has argued that social changes mean that privacy is no longer a norm [9]. The privacy issues cropped up by the technology cannot be resolved by

[1] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-182-3

applying traditional approach to right to privacy. This is the reason that the privacy jurisprudence was revisited in the light of the developments that took place by the introduction of Internet. The right to privacy is now loaded with fresh contents and it is contended that its breach would include: a) information collection, consists of surveillance and interrogation, b) information processing, involves taking the information gathered and making sense out of the raw facts for any probable use which can be further classified into aggregation, identification, insecurity, secondary use and exclusion, c) information dissemination, concerned with the dissemination of the information and it consists of the breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion, and d) invasion, concerning invasive acts that disturb one's tranquility or solitude without concerning information [10].

In digital age, breach of privacy cannot be properly addressed if it is circumscribed by 'the right to leave alone.' Privacy is about knowing 'what data is being collected' and 'what is happening to it', having choices about how it is collected and used, and being confident that it is secure.[2]

The importance of marketable information has been so profound that it is argued that privacy as a fundamental concept should extend its reach to 'information privacy' for online transactions and personally identifiable information [11] that would include an individual's claim to control the terms under which 'personal information' is acquired, disclosed, and used.[3]

II. Indian Constitutional Approach to Privacy

The right to privacy as a fundamental right was accorded recognition in India much before the Independence of India and adoption of the Indian Constitution. The Allahabad High Court in *Nihal Chand* v.*Bhawan Dei*[4] made the following pertinent observation:

'The right to privacy based on social custom is different from a right to privacy based on natural modesty and human morality, the latter is not confined to any class, creed, colour or race and it is birth right of any human being and is sacred and should be observed.'

The right to privacy as a fundamental right has not been expressly mentioned in the Indian Constitution. The courts in India have stretched Article 21[5] to encompass right to privacy as a fundamental right by holding that right to life means a dignified life. This right to privacy like other fundamental rights is not an absolute right but admits reasonable restriction.

The Supreme Court of India has, immediately after the adoption of the Constitution, laid down foundation for privacy jurisprudence in *M P Sharma* v. *Satish Chandra*[6]. It was held that a power of search and seizure is in any system of State for the protection of social security and the power is necessarily regulated by law. This positive approach was carried further in *Kharak Singh* v. *State of UP*[7] by J. Subba Rao, the architect of modern privacy Jurisprudence. The Apex court found seeds of privacy jurisprudence in Article 21 and held that this Article is comprehensive enough to include right to privacy. The pertinent observation, valid for all times to come, is that a person's house, where he lives with his family is his "castle" and nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy. This right was further fortified in *Gobind* v. *State of MP* [8]by accepting limited recognition in Articles 19(a)(d) in addition to Article 21. While expanding horizons of privacy jurisprudence, the Supreme Court held that right to liberty, right to move freely throughout the territory of India and the freedom of speech taken together create an independent right to privacy. In the words of Justice Mathews, the fundamental rights explicitly guaranteed to a citizen have penumbral zones and the right to privacy is itself a fundamental right. The apex court formulated the following principles to govern the right to privacy:

a) Privacy – dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior,
b) If the court does not find that a claimed right is entitled to protection as a fundamental right, a law infringing it must satisfy the compelling state interest test,
c) Privacy primarily concerns the individual. It therefore relates to and overlaps with the concept of liberty,
d) The most serious advocates of privacy must confess that there are serious problems of defining the essence and scope of the right. Privacy interest in autonomy must also be placed in the context of other right s and values, and
e) Any right to privacy must encompass and protect the personal intimacy of the home, the family, marriage, motherhood, procreation and child rearing.

Malak Singh v. *State of Punjab*[9] represents an extended reach of privacy jurisprudence. The apex court held that a surveillance of the subject by the state is intrusive and an encroachment upon his right to privacy. This approach was taken to new heights by the Indian Courts in a number of cases[10].

[2] Testimony of Mr. Erich Anderson, Deputy General Counsel of Microsoft Corporation, *The State of Online Consumer Privacy, Hearing before S. Comm. on Commerce, Science, and Transportation*, 112th Cong., (2011) (hereinafter Microsoft testimony)

[3] U.S. Govt. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, Commentary 2 (1995)

[4] AIR 1935 All. 1002

[5] Article 21, "Protection of Life and Personal Liberty" No person shall be deprived of his life or personal liberty except according to procedure established by law.

[6] AIR 1954 SC 300

[7] AIR 1963 SC 1295

[8] (1957) 2 SCC 148

[9] (1981)1 SCC 301

[10] See for instance, *PUCL* v. *Union of India*. AIR 1991 SC 207; *State of Maharashtra* v.*Madhukar Narayan Mordikar*, AIR 1999 SC 495; *Mr.X* v. *Z Hospital*, (1998) 8S CC 996; *R. Rajagopal* v. *State of Tamil Nadu*, AIR 1995 SC 264; *District Registrar and Collector* v. *Canara Bank* AIR 2005 SC 186

On technology front, the apex court found an opportunity more than once to pronounce that the privacy right exists even when the technology is used to circumvent this right. In *R.M. Malkani* v. *State of Maharashtra*[11] the apex court held that the telephonic conversation of an innocent person would be protected by the courts against wrongful or high handed interference by tapping of the conversation by the police. A more elaborative approach was adopted by the apex court in *Peoples Union for Civil Liberties* v. *Union of India*[12]. It was held that the telephonic tapping, a form of technological eavesdropping, infringes the right to privacy. Justice Kuldeep Singh laid down that the telephone taping which amounts to intrusion into privacy can take place only in the gravest of grave situation when national security is endangered and not otherwise. In usual or normal circumstance, there should not be any phone tapping and the person should not be under surveillance because he has right to privacy, which is a part of the right to life and is recognized by the constitution of India.

III. Limits of Privacy Right

The courts in India have maintained that like other fundamental rights, the right to privacy is not absolute. This right cannot be claimed where the information sought to be published or disseminated is already in public domain[13] or there is reasonable excuse available. This right to privacy is available only against the State and not against any private individual[14]. In a more recent case of *State of Maharashtra* v. *Bharat Shanti Lal Shah*[15], the apex court observed that "interception of conversation though constitutes an invasion of an Individual's right of privacy but the said right can be curtailed in accordance with procedure validly established by law. Thus, what the court is required to see is that the procedure itself must be fair, just and reasonable and non-arbitrary, fanciful or oppressive.

IV. Judicial Approach to Privacy in Cyberspace

Indian judiciary has not yet found an opportunity to deliberate on the privacy issues associated with cyberspace but there are instances in transnational jurisdictions where courts have authoritatively invoked privacy right in cyberspace. In America, the Supreme Court in *Whalen v. Roe*, [16] recognized an implicit constitutional right of informational privacy. A New York law empowered to create a centralized state computer file of the names and addresses of all persons who obtained medicines containing narcotics pursuant to a doctor's prescription. The Court upheld the validity of the law, nevertheless, it held that this gathering of information impinges upon two interests. The first was an individual interest in avoiding disclosure of personal matters; the other, the interest in independence in making certain kinds of important decisions. These two interests rest on the substantive due process protections found in the Fifth and Fourteenth Amendments.

The courts in America have in a good number of cases upheld in different contexts citizen's right to privacy in cyberspace. In *US v. Ziegler*, [17] an employee had accessed child pornography websites from his workplace. His employer noticed his activities, made copies of the hard drive, and gave the FBI the employee's computer. At his criminal trial, Ziegler filed a motion to suppress the evidence because he argued that the government violated his Fourth Amendment rights.

The Ninth Circuit allowed the lower court to admit the child pornography as evidence. After reviewing relevant Supreme Court opinions on a reasonable expectation of privacy, the Court acknowledged that Ziegler had a reasonable expectation of privacy at his office and on his computer. That Court also found that his employer could consent to a government search of the computer and that, therefore, the search did not violate Ziegler's Fourth Amendment rights.

The New Jersey Supreme Court held in *State v. Reid* [18] that computer users have a reasonable expectation of privacy concerning the personal information they give to their ISPs. This case also serves as an illustration of how case law on privacy regarding workplace computers is still evolving.

In *Robbins v. Lower Merion School District* [19] (U.S. Eastern District of Pennsylvania 2010), the federal trial court issued an injunction against the school district after plaintiffs charged two suburban Philadelphia high schools violated the privacy of students and others when they secretly spied on students by surreptitiously and remotely activating webcams embedded in school-issued laptops the students were using at home. The schools admitted to secretly snapping over 66,000 web-shots and screenshots, including webcam shots of students in their bedrooms.

In a recent decision [20] , the Court reconfirmed its recognition of a constitutional right to information privacy. The contract workers of National Aeronautics and Space Administration (NASA) contended they are required to answer questions about their drug treatment and are asked their references whether they have any reason to question the

[11] AIR 1973 SC 157.

[12] AIR (1997) 1 SCC 301.

[13] In *Petronet LNG Ltd.* v. *Indian Petro Group*, (2009) 95 S.C.L. 207 (Delhi) (India) the case concerned an application for an injunction against the defendants from publishing information which the plaintiff alleged was confidential. The plaintiff alleged that the defendant breached its privacy by accessing as well as disseminating information. The court held that the information was freely available in public and hence the defendant was not in breach of the plaintiff's right to privacy; Similarly in *Rajinder* Jaina v. *Central Information Commission*, 164 (2009) D.L.T. 153 the case concerned a writ petition about the disclosure of information under the Right to Information Act, 2005 wherein the petitioner challenged the disclosure on grounds of infringement of the right to privacy. The court held that the information already existed in the public domain and no claims as to privacy could be made.

[14] *See, Khushwant Singh* v. *Maneka Gandhi*, A.I.R. 2002 Del. 58; Indu Jain v. Forbes Incorporated, IA 12993/2006 in CS(OS) 2172/2006 (High Court of Delhi, 12th October 2007) (India). The court noted that the enforcement of the right to privacy under the Indian constitutional scheme can only be made against state instrumentalities and not against private persons.

[15] (2008) 13 S.C.C. 5 (India) (*Per* K. G. Balakrishnan, C. J. et al.).

[16] 429 U.S. 589 (1977)

[17] F.3d 1077 (9th Cir. Jan. 30, 2007, No. 05-30177)

[18] lawlibrary.rutgers.edu. Retrieved 2011-11-25

[19] Doug Stanglin (February 18, 2010). "School district accused of spying on kids via laptop webcams". USA Today. Retrieved February 19, 2010.

[20] 131 S. Ct. 746 (2011)

individual's honesty or trustworthiness. NASA thus violated their privacy rights under the U.S. Constitution. The court rejected this contention 8-0. The court recognized individual's right to informational privacy but also recognized Government's legitimate interest and held that the Government is not precluded from taking reasonable steps to serve its legitimate interests for public good.

V. Technological Approach to Privacy in India

Recent measures for the fight against terrorism and organized crime do stipulate serious interference with common human rights - particularly in form of monitoring and interception of information of individuals in India. There has been a constant debate about the supremacy of individual's fundamental right and the state's sovereign power to maintain security and in turn integrity of the country. This debate has sharpened after 9/11 in America [12] and 26/11 in India. The Governments have given legal mandate to the use of technology for monitoring and surveillance. The Indian Government framed Rules in April, 2011 asking Internet service providers to delete information posted on websites that officials or private citizens deemed disparaging or harassing. The Government also plans to set up its own unit to monitor information posted on websites and social media sites. (Govt. faceoff brewing with Facebook, others, Times of India, 5th December, 2011)

The growing interest in the new surveillance technology is precisely due to the fact that these technologies have enormously increased government's capacity to develop record keeping instruments and refined instruments of control that often impinges upon the privacy and other associated rights. This has resulted in the enactment of Data Protection laws in many countries that are based on the premise that autonomous fundamental right have to be preserved in all levels that involve personal data processing for private or public aims but there may be situations in which states can deny right to privacy in public good and counter terrorism is one of them for the aims of which security agencies can investigate and check persons or personal belongings also with new technological systems. However, counter terrorism, in no case can legalize all the interferences in the private spheres of individuals. There has to be reasonable nexus between the means and the objective to be achieved [13]. After all, a decent treatment of people in society represents a core value of data protection, and implies that people know when and for what purpose their data are collected. This may, however, prove a high degree of privacy protection especially in the present Indian context as is evinced by the following provision of the IT Act.

A. Power to Decrypt Information

Prior to Amendment Act, 2008, the Controller of the Certifying Authorities had power to decrypt any information in the interest of sovereignty, security, and integrity of the country. This power has been taken from the Controller and is given to the Central or State Government or any of its officers especially authorized by the Central or State Government as the case may be. From mere power of the Controller to decrypt information, the Central Government or the State Government has enormous powers which include:

a) Power to intercept, monitor, or decrypt any information, and
b) Power to monitor and collect traffic data or information.

B. Power to Intercept, monitor or decrypt any Information

The Central or State Government or any of its officers who has been specially authorized by the Central or State Government as the case may be, may direct any agency of the appropriate Government to intercept or monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource[21]. The term 'decryption' means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof[22].

The word 'intercept' with its grammatical variation and cognate expressions means aural or other acquisition of the contents of any information through the use of any means, including an interception device, so as to make some or all of the contents of information available to a person other than the sender or recipient or intended recipient of that communication, and includes:

a) Monitoring of any such information by means of any monitoring device,
b) Viewing, examination or inspection of the contents of any direct or indirect information, and
c) Diversion of any direct or indirect information from its intended destination to any other destination.[23]

The word 'monitor' with its grammatical variations and cognate expressions, includes to view or to inspect or listen to or record information by means of a monitoring device[24].

The above power is not limitless. It can be exercised only when the authority empowered is satisfied that it is necessary or expedient so to do, in the interest of:

a) Sovereignty of India, or
b) Integrity of India, or
c) Defense of India, or
d) Security of the State, or
e) Friendly relations with the foreign States, or Public order, or
f) For preventing incitement to the commission of any cognizable offence relating to above, or
g) For investigation of any offence.

Before any order is issued under this provision, the competent authority has to record reasons in writing for making such order. The competent authority for this purpose means:

a) The Secretary in the Ministry of Home Affairs in case of the Central Government, or

[21] Section 69 of the IT Act

[22] Rule 2 (f) of the IT Act (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009

[23] Rule 2 (i) (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009

[24] Rule 2 (o) (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009

ISBN: 978-1-61208-182-3

b) The Secretary in charge of the Home Department, in case of the State Government or the Union territory as the case may be.[25] The competent authority may call any subscriber or intermediary or any person in-charge of the computer resource that shall extend all facilities and technical assistance to:

- Provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information, or
- Intercept, monitor, or decrypt the information, as the case may be, or
- Provide information stored in computer resource.

The subscriber or intermediary or any person who fails to assist the competent authority shall be punished with imprisonment for a term which may extend to seven years and shall be also liable to fine. The term intermediary with respect to any particular electronic record means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.[26]

The above provision finds parallel in Section 5(2) of the Telegraph Act that has been framed in pursuance to the Supreme Court pronouncement in *PUCL v. Union of India*[27]. These rules provide when a) public emergency, or b) public safety situation exists, then an order may be made to issue directions for interception. These rules effectively authorize to issue directions for the interception of messages. A balancing measure to safeguard against a blanket violation of privacy has been provided. The section itself provides for several safeguards that include recording of reasons for taking any of these steps. These measures cannot be taken unless it is shown that such step is necessary or expedient in the interest of a) sovereignty and integrity of India, b) the security of the state, c) friendly relations with foreign states, d) public order, and e) incitement to the commission of an offence. There is no direct case decided by any court in India on the above issue. However, recently the United States court of Appeals for the district of Columbia Circuit in Appellee vs. Lawrence Maynard[28] had an opportunity to decide effect of use of GPS on privacy right of an individual. The court observed that the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave. A search conducted without a warrant is per se unreasonable under the fourth amendment subject only to a few specifically established and well delineated exceptions. The court gave go ahead to the use of technology for surveillance purpose for security reasons subject to certain safeguards.

C. Procedure for Interception, Monitoring, or Decryption of any information

The circumstances warranting interception, monitoring and decryption of information can be classified into three categories, namely: a) Normal, b) unavoidable, and c) Emergency[29]. The interception, monitoring, or decryption of any information can be carried out in normal circumstances only by an order issued by the competent authority. No person shall carry out the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource, except by an order issued by the competent authority. The interception, monitoring, or decryption of any information can be carried out in unavoidable circumstances by an officer not below the rank of the joint secretary to the Government of India, provided that he has been duly authorized by the competent authority.

Emergency cases have been subdivided into two categories: a) Locational, and, b) operational. The interception, monitoring, or decryption of any information may be required in a remote area but obtaining of prior directions for such interception or monitoring or decryption of information is not feasible. Or where obtaining of prior directions for interception or monitoring or decryption of any information generated, transmitted, received or store in any computer resource, for operational reasons, is not feasible.

In the emergency cases, resulted by locational or operational reasons, the interception, monitoring, or decryption of any information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or the second senior most officer of the security and law enforcement agency at the central level and the officer and the officer authorized in this behalf not below the rank of Inspector General of Police or an officer of equivalent rank at the State or Union territory level.

The officer, who has permitted the interception, monitoring, or decryption of any information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception, monitoring, or decryption within three days. The concerned officer must obtain the approval of the competent authority within the period of seven working days. If the approval of the competent authority has not been obtained within the stipulated time of seven working days, such interception, monitoring, or decryption shall cease and the information shall not be intercepted, monitored or decrypted thereafter without the prior approval of the competent authority.

It is quite possible that the State Government or Union Territory administration may require interception, monitoring, or decryption of any information beyond its territorial Jurisdiction. The Secretary in-charge of the Home Department in that State or Union Territory, as the case may be, shall make a request to the secretary in the Ministry of Home Affairs, Government of India for issuing direction to

[25] Rule 2 (d) of the IT Act (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009

[26] Section 2 (w) of the IT Act

[27] Supra note 12

[28] No. 08-0330 decided on August 6, 2010

[29] Rule 3 of the IT Act (Procedure and Safeguard for Interception, Monitoring and Decryption of Information) Rules, 2009

the appropriate authority for such interception, monitoring, or decryption of information.

The competent authority shall consider possibility of acquiring the necessary information by other means and the direction shall be issued only when it is not possible to acquire the information by any other reasonable means.

Every direction shall specify the name and designation of the officer of the authorized agency to whom the intercepted, monitored or decrypted information shall be subject to the provisions of the IT Act. The direction for interception or monitoring or decryption shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of its issue and may be renewed from time to time for such period not exceeding the total period of one hundred and eighty days.

The above provisions have been incorporated by the Amendment Act, 2008 and attempt to remove the limitations of the original Act by making IT Act a complete code for Internet behavior. This provision, like Section 69 has roots in the ratio of *PUCL v. Union of India*[30] wherein the court has held that the direction may only be issued when it is warranted by a) public emergency; or b) public safety. These limitations are based on Section 5(2) of the Telegraph Act. The direction must contain reasons for taking such measures. It also contains the requirement of recording for which the prescribed procedure under section 69(2) has to be followed.

VI. Criminal Liability for Violation of Privacy

The IT (Amendment) Act has carved out a new provision which makes capturing of an "image of the private area of a person", under circumstances violating the privacy of the person, punishable. The circumstances violating the privacy of a person are when such person has a reasonable expectation that a) he or she could disrobe in privacy without being concerned that an image of his/her private area was being captured, or b) any part of his/her private area would not be visible to the public, whether such person is in a public or a private place.[31] Where a person lawfully secures access to any electronic record, book, register, correspondence, information, document or other material and discloses such electronic record, book, register, correspondence, information, document or other material to any other person without the authority of the person concerned, he shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one lakh rupees or both.[32] But surprisingly there is no provision for imprisonment or fine for simple breach of privacy committed by an individual.

VII. Conclusion

India has no independent legislation on Data Protection. The existing legal principles are yet to be tested in cyberspace as the courts have not yet found any direct opportunity to decide any case involving privacy issues of cyberspace. The only inference which one could draw from the existing precedents involving other technologies is that courts are stressing on procedural safeguards and are shying away from establishing substantively limits of the state's power to circumvent right to privacy. The IT Act has laid down procedure for interception, monitoring and decryption of the information and imposed criminal liability on any person who captures image of the private part of any person. Similarly, any person who has got information lawfully but discloses it without the authority of the person concerned will be punished but there is no provision for imprisonment or fine for simple breach of privacy committed by an individual.

References

[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4 Harv.L.Rev. 193 (1890).

[2] William L. Prosser, "Privacy", CAL. L. REV., 48, (1960), pp. 383.

[3] Monteleone, Share, "Ambient Intelligence and the Right To Privacy: The challenges of Detection Technologies," European University Institute, DOI:10.2870/24183.

[4] S. Gutwirth, "Biometrics between Opacity and Transparency," Annuali dell'Istituto Superiore di Sanita, 43(1), (2007), pp. 61-65.

[5] Lipton, J. D., "Mapping Online Privacy," Case Western Reserve University School of Law, Case Research Paper Series in Legal Studies Working Paper (2009), pp. 09-24.

[6] Shrikant Ardhapurkar et al. "Privacy and Data Protection in Cyberspace in Indian Environment," International Journal of Engineering Science and Technology, 2(5), (2010), pp. 942-951.

[7] O'Hara, K. and Shadbolt, N., "The Spy in the Coffee Machine: The End of Privacy As We Know It," One-world, Oxford, (2008).

[8] Jacqueline D.L., "Mapping Online Privacy," 477 N.W. U. L Rev., 140, (2010), pp. 481-82.

[9] Johnson, B., "Privacy no longer a social norm, says Facebook founder," Guardian, 11th Jan, (2010).

[10] Daniel J.S., "A Taxonomy of Privacy," 154 U. PA. L. REV., 477, (2006), pp. 482-483.

[11] Joel R.R., "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights? ," 44 Fed. Comm. L.J. (1992), pp. 195.

[12] Zuac L., "Constitutional Dilemmas," Oxford University Press, (2008).

[13] Van Der Schyff, G., "Limitation of Rights," Wolf Legal Publisher, Nijimegen, (2005), pp. 228.

[30] Supra note 27

[31] Section 66E

[32] Section 72

ISBN: 978-1-61208-182-3

Cloud Computing and Data Jurisdiction: A New Challenge for Digital Forensics

Giuseppe Vaciago
Faculty of Law
University of Milan
Piazza Ateneo Nuovo 1, Milan, Italy
e-mail: vaciago@htlaw.it

Abstract— **Although it has become clear that digital forensics – the practical analysis of digital data following the acquisition of a bit-stream image of a suspect's hard disk – suffered a setback with the wide adoption of mobile devices and the increasing use of flash memory and encryption systems, it is undoubtedly also the case that it experienced a fundamental change due to the incredible expansion of cloud computing systems. In this article, the aim is to study the jurisdictional problems that cloud computing systems cause and the possible solutions at an EU level that have been adopted by legislators and the courts of the European Union in relation to the gathering of digital evidence that may be concealed in the 'clouds'. Particular attention must be paid to German and Italian case law experience as Courts in these countries have addressed the problem, providing different solutions to resolve the same problem.**

Keywords: **Cloud Computing; Digital Forensics; Remote Forensics; Jurisdiction.**

I. INTRODUCTION

The increasing popularity of cloud computing [1], moreover, has made conventional crime detection even more difficult: the very strengths of cloud computing, which allows anyone anywhere in the world to use publicly accessible software to process data stored in a virtual cyberspace location, could be put to devious use by criminals to store incriminating data on a server located beyond the jurisdiction of the courts of their country of residence, preferably in a State with no judicial cooperation treaty with that country.

Over the last few years, various approaches have been offered to solve the 'loss of location' of digital evidence in the 'cloud world'. The traditional approach is the territorial principle by virtue of which the court in the place where the data is located has jurisdiction. This approach essentially prohibits any type of investigation because even the cloud provider might not know exactly where the data is located.

Another approach is the nationality principle by virtue of which the nationality of the perpetrator is the factor used to establish criminal jurisdiction. This principle imposes certain restrictions, since the perpetrators in a cybercrime case might easily be foreign nationals, given that cybercrime is generally transnational and there is no need for physical proximity. Furthermore, data does not have a nationality, because it is an attribute of an individual.

A third approach is the 'flag principle', which basically states that crimes committed on ships, aircraft and spacecraft are subject to the jurisdiction of the flag State, regardless of their location at the time of the crime (article 22, Convention on Cybercrime) [2]. Since digital data is constantly changing, this principle also seems to be applicable to cloud computing. However, to apply this to the cloud computing scenario, it is necessary to remember that this principle could motivate cybercriminals to select a cloud computing provider under a 'pirate flag'.

Finally, a recent discussion paper, prepared by the Council of Europe within the framework of the global Project on Cybercrime, suggested the 'Power of Disposal Approach' [3]. From a practical point of view, a regulation based on the power of disposal approach would make it feasible for law enforcement to obtain access to a suspect's data within the cloud. Law enforcement would only have to legally obtain the username and password combination and be able to prove that additional requirements have been met. This type of approach certainly overcomes any jurisdictional issue, but a balance must be struck with the legitimate need for privacy and the rights of the citizens even if a judicial authority investigates them.

There has been heated debate on both sides of the Atlantic in recent years on the wisdom of empowering law enforcement authorities to use remote forensics technology to obtain access to the digital data storage devices (laptops, serves, smart telephones, etc) of suspects. Law enforcement agencies find it increasingly difficult to locate the servers on which incriminating data are stored, since perpetrators tend to rely on remote access connections to store and process data using faraway devices [4].

II. LEGISLATIVE MEASURE OF THE CONVENTION ON CYBERCRIME

To overcome obstacles generated by the 'data loss' location of digital evidence, signatory States have endowed their respective judicial authority and law enforcement agencies with a number of legislative measures in implementation of articles 18 (Production Orders), 19 (Search and Seizure of Stored Computer Data) and 20 (Real-time Collection of Traffic Data), of the Convention on Cybercrime.

Under article 18 of the Convention on Cybercrime, signatory States are required to empower their respective judicial authorities to issue Production Orders requiring any person or party (obviously, including ISPs) to submit to law enforcement authorities specific digital data in the possession or control of the person or party in question, and stored on a computer system or data storage medium [5].

Some Italian commentators hold the view that Production Orders could also be issued to compel the disclosure of data pertaining to web users based outside the boundaries of a signatory State, provided that the same have signed up for services provided by an ISP that operates, amongst other things, in the signatory State in question [6].

This interesting approach appears, however, to conflict with the principle of sovereignty, and, may, in any event, be applied solely to subscriber information (article 18(1)(b) of the Convention on Cybercrime), since only ISPs located within the territory of the signatory State in which the Production Order is issued may be compelled to submit user-generated content (article 18(1)(a) of the Convention on Cybercrime) [7].

Pursuant to article 19 of the Convention on Cybercrime, moreover, signatory States are required to ensure that, upon discovering that pertinent digital evidence is, in fact, stored on another server, their respective law enforcement agencies are also empowered to access also the other server, provided, however, that the latter is located within their national borders, and that the digital data to be seized, may be accessed from the server initially covered by the related search and seizure warrant.

In any event, even when searching for specific data stored on a computer system located within the borders of the signatory State in which the Production Order is issued, law enforcement agencies may encounter serious difficulties as a result of the sheer volume of data to be parsed to find useful digital evidence.

In light of these obstacles, the Convention on Cybercrime requires law enforcement agencies to be empowered to compel the IT manager to provide 'as is reasonable' the information necessary for successfully securing the digital evidence sought [8].

Finally, article 20 of the Convention on Cybercrime requires that law enforcement authorities of signatory States to be afforded real-time access to web traffic data, that is to say the electronic records of a suspect's on-line activities (web sites visited, e-mail correspondents, downloads, etc).

Towards this end, signatory States must enact national legislation requiring ISPs either to provide law enforcement authorities with the software tools necessary for directly collecting and recording traffic data subject to search and seizure, or alternatively, to collect and record such data on an ad hoc basis, pursuant to a judicial or prosecutorial order to such effect.

As in the case of evidentiary seizures of e-mail, 'Production Orders' and the 'Real-time Collection of Traffic Data' contemplated in articles 18 and 20 of the Convention on Cybercrime respectively, are very similar to the interception of communications, which are subject to specific restrictions pursuant to article 8 of the European Convention on Human Rights.

Sadly, these three crucial 'crime-fighting' tools, entrenched in the Convention on Cybercrime, are available only in part to Italian law enforcement agencies. Whilst the Italian Code of Criminal Procedure does, in fact, currently contemplate procedural instruments designed to achieve the same results (the appointment of a digital forensics expert to assist law enforcement officers pursuant to article 348, paragraph 4; discovery orders within the meaning of article 248; and interception of communications regulated under article 266-*bis*), in ratifying the Convention on Cybercrime, Italy failed to avail of a significant opportunity to fine-tune these 'crime-fighting tools'.

III. ITALIAN AND GERMAN CASE LAW ON REMOTE FORENSICS TECHNOLOGY

Several European countries are currently considering legislation that would invest their law enforcement authorities with powers to remotely monitor and record the traffic data of suspects in real time to an extent that far exceeds the scope of the procedural tools outlined above [9], whilst, on the other shore of the Atlantic, the FBI has already successfully tested a peculiar type of spyware (CIPAV) specifically designed for such a purpose [10].

In any event, it is clear that by allowing law enforcement officers to monitor the on-line activities of a blissfully unaware suspect from the air-conditioned comfort of their offices, remote forensic techniques have proven far more cost-efficient and effective than conventional detective work and, moreover, without any jurisdictional problems, as digital evidence would not be acquired in a territory other than the one in which the Prosecutor has jurisdiction.

At the same time, it would be perilous to lose sight of the dangers that such invasive techniques might entail in terms of the citizen's fundamental rights and freedoms. Great care must, accordingly, be taken to properly weigh all the legal interests involved, and strike a delicate balance between the prevention of crime and public security, and the need to protect the suspect's due process, privacy and other human rights.

On this issue, it is interesting to note that the Italian Supreme Court evinced no need to address the constitutionality of a prosecutorial warrant, authorizing the use of surreptitiously installed ghost software to obtain a copy of the digital data stored on a desktop used by the suspect and located in a public office on the grounds that the related evidentiary seizure order did not pertain to a flow of communications but merely entailed the mining of data already stored on the suspect's desktop, that is to say, a 'a one-directional flow of data' contained within the computer's internal circuitry [11].

The Supreme Court moreover held that, in the case in question, this technical activity was repeatable, given that 'copying the stored files neither altered the same nor entailed the destruction of the database which remained totally unchanged, and therefore accessible and open to consultation, subject to the same terms and conditions, even upon conclusion of evidence gathering operations'.

According to the Supreme Court, the copying in question amounted to no more than a repeatable operation that could be undertaken without informing defense counsel, much less inviting the latter to attend the proceedings, since the same operation could be reproduced and repeated a second time if need be for procedural purposes, although such need did not arise.

During the Supreme Court proceedings, however, counsel for the defense argued that the warrant issued by the public prosecutor, whilst authorizing no more than the seizure of a copy of the digital data in question, effectively entailed the interception of computerized communications. The scope of the prosecutorial warrant, in fact, covered not only the files already stored in the suspect's computer system through to the date of the related search and seizure, but also any and all data input into the system in the future.

This factual situation was confirmed by the operating procedures followed in executing the prosecutorial warrant, which included the surreptitious installation of ghost software on the computer system in question, for the purpose of copying files already stored on the computer, and subsequently copying in real time any and all data processed using the computer system, before, finally, transmitting all the data that was copied back to law enforcement officers on a periodic basis. As a result, the computer system used by the suspect was effectively subjected to digital surveillance for over eight months.

The ruling deserves criticism from two standpoints: first, the Supreme Court does not appear to have considered the fact that the alleged repeatability of the copying and transmitting operations necessarily implies that no further data processing was carried out using the computer system in question, following the original operations; second, in support of its refusal to apply the statutory provisions regulating the interception and recording of communications, the Supreme Court goes no further than to point out that the flow of communications copied by and transmitted to law enforcement authorities did not pertain to electronic correspondence between two private parties, but focused solely on a 'unilateral flow of communications'.

Whilst this approach is certainly reasonable, there still seems to be a cloud of mystery shrouding both the Supreme Court's refusal to apply article 266-*bis* which regulates the interception of a 'flow of communications pertaining to computerized or electronic systems, or otherwise among several systems', and its apparent tolerance of highly invasive evidence-gathering techniques that go so far as to entail the prolonged monitoring of a computer system without judicial oversight.

A totally different approach was taken by Germany. On 20 December 2006, article 5.2 (11) of the Law on the Protection of the Constitution in North Rhine-Westphalia was amended with the introduction of provisions on remote forensics instruments, both on-line and by obtaining access to information technology systems [12].

The issue first came to the attention of the general public and legal scholars in 2006 when a state prosecutor applied to the Federal Court of Justice of Germany (Bundesgerichtshof) to authorize a remote search of computers allegedly containing data useful to continuing investigations, by applying an analogy to the law governing search-and- seizure operations conducted on physical premises. The court dismissed the motion, holding that clandestine remote searches of computers could not be deemed analogous to raids conducted on physical premises, but left open the possibility for new laws to be enacted endowing law enforcement authorities with specific search-and-seizure powers in respect of electronic data. It was this latter portion of the decision that led to the amendment of the Law on the Protection of the Constitution in North Rhine-Westphalia.

The new provisions reinforced the domestic secret service known as the 'Federal Office for the Protection of the Constitution' (Bundesamt für Verfassungsschutz) by authorizing the establishment of an agency with the specific task of gathering intelligence by obtaining covert access to computer systems and secretly monitoring on-line communications and web traffic.

Private computer systems could be covertly accessed either physically, using hardware (interception of communications and bugs) or 'remotely', thanks to software (keylogger and sniffer programs) installed on the target system without the owner's knowledge, for instance, in the form of Trojans incorporated within or disguised as harmless content, by convincing the hapless owner to voluntarily upload the relevant spyware or disclose passwords through cleverly devised social engineering and phishing initiatives [13].

Under the amendment in question, the above remote forensics operations could be launched without a warrant or court order of any kind, and there was no specified limit on how long a particular computer system and on-line communication could be subjected to surveillance.

In consideration of all these elements, the German Constitutional Court [14] determined that the constitutionality of the amendment had to be assessed in light of three distinct fundamental rights enshrined in the country's Basic Law (Grundgesetz – GG): the privacy of correspondence [15], the inviolability of the home [16] and the 'right to informational self-determination' [17].

With regard to the privacy of correspondence, the Constitutional Court held that this fundamental privilege extended to all types of telecommunications regardless of the means of transmission used (cable or broadcast, analog or digital transmission), and the type of transmitted content (speech, picture, sound, or other data). However, the court went on to assert that constitutional protection did not extend to telecommunications data stored on computerized devices after the communications process had been completed. In effect this means that it is not unlawful for the German secret service to surreptitiously copy data from the computer hard drives of suspects.

With regard to the second fundamental right engaged in the case, the Constitutional Court pointed out that the principle of the inviolability of the home, enshrined in article 13.1 of the Basic Law, only bars law enforcement officers from trespassing on private property in a bid to physically interfere with the hardware located on the premises. Since remote surveillance using Trojans or other spyware can be conducted regardless of where the target device may be located at any given time, location-specific protection falls far short of ensuring adequate safeguards, especially since it is increasingly commonplace for computers to be operated outside or in transit between private premises.

Finally, the Constitutional Court examined the amendment in light of the ‘right to informational self-determination’ which protects web users against the collection and profiling of the data they post on-line. Once again, however, the remote forensics activities authorized under the amendment to the Law on the Protection of the Constitution go beyond the mere collection of personal data for profiling purposes, since clandestine access to just about any personal computer could, on its own, potentially prove a valuable discovery of highly sensitive data regarding its owner, without the need for any further profiling of the information collected in the process.

Having determined that the three fundamental rights enshrined in Germany’s Basic Law afforded inadequate protection in the circumstances, the Constitutional Court opted to establish a new ‘right to the confidentiality and integrity of information technology systems’.

In the same way as the ‘right to informational self-determination’, this new ‘right to the confidentiality and integrity of information technology systems’ can be found in article 2.1 GG (right to the free development of one’s personality), read in conjunction with article 1.1 GG (right to human dignity) and provides protection against State access to each and every information technology system taken as a whole, and therefore extends to all data, whether stored or transmitted.

Although the court conceded that the right to the confidentiality and integrity of information technology systems is not absolute and may be restricted in the interest of law enforcement and crime prevention, it took pains to point out that no encroachments on the newly created constitutional right could be tolerated, save to the extent necessary to safeguard even more imperative fundamental values which the court specifically limited to the life and liberty of other citizens, the foundational institutions of the State and the essential values of human dignity.

IV. CONCLUSION

While declaring the amendment unconstitutional by reason of breach of the principles of proportionality and fair labelling, the German Constitutional Court has, however, left room for the passage of new laws authorizing remote forensic and on-line surveillance operations, albeit within the bounds of the principles outlined above.

It has, quite rightly, been pointed out that ‘the digital citizen has, as a result of this case, come a step closer’: there can be no doubt that an increasing number of individuals not only use web technology on a daily basis, but actually ‘live’ on-line. The internet has become a place where people make friends, come together and exchange information and opinions. The German Constitutional Court acknowledged that the pre-existing legal framework was not robust enough to adequately protect ‘digital’ citizens against unwarranted State intrusion.

More intriguing, however, are the comments on the decision by German authors who posit that software programs themselves could be considered invested with rights, freedoms and duties, and subjected to monitoring in accordance with applicable procedural requirements, quite like people [18].

At present, Trojans are considered mere software tools used by law enforcement officers to prevent, solve, fight and thwart crime. What if, tomorrow, the courts were to consider Trojan fully-fledged ‘digital police officers’ who inhabit cyberspace on an equal footing with ‘digital citizens’?

To engage in this thought experiment is to follow Alice as she steps through the looking-glass – or rather the computer screen – to enter a Wonderland whose cyber-inhabitants enjoy the same rights and freedoms and are bound by the same ethical rules and duties as citizens in the real world, with the full complexity of self-perception and overall vision of the virtual community and its peculiar social norms, that the human beings behind the cyber-personalities or software programs actually experience online.

The implementation of any such virtual legal system, would obviously require a complete overhaul of prevailing philosophies of law, and entail deep-reaching legislative reforms tailored to suit the worldview of the growing international community of people who work, relax, study, play, and socialize largely online.

In such a scenario, it would be quite useless to train law enforcement officers in digital forensics, and far more sensible to develop software applications designed specifically to police the borderless confines of cyberspace, and endowed with computational capabilities to match the performance levels of the virtual citizens subject to their authority. These policing software applications would have

ISBN: 978-1-61208-182-3

to be developed by computer-science specialists who are also well-versed in the finer points of law (especially criminal procedure), and, consequently, necessarily entail a multidisciplinary approach.

To conclude, my opinion is as follows: remote access to an IT system situated in the location where the prosecutor conducting investigations has jurisdiction makes it possible to solve the "data loss" location problems. However this type of activity must be carried out fully respecting the constitutional guarantees of the person under investigation and people having multidisciplinary skills, legal and technical alike must conduct it.

REFERENCES

[1] Janna Quitney Anderson and Lee Rainie, "The Future of cloud computing", *Pew Internet & American Life Project*, 11 June 2010, available at http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx.

[2] Article 22 of the Convention on Cybercrime (Jurisdiction): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: (a) in its territory; or (b) on board a ship flying the flag of that Party; or (c) on board an aircraft registered under the laws of that Party; or (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State [….].

[3] Jan Spoenle, "Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?", (31 August 2010, Council of Europe Project on Cybercrime), available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf.

[4] Dr Marco Gercke, "Understanding Cybercrime: A Guide For Developing Countries", (April 2009), 192, available at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html.

[5] Orin S. Kerr, "Searches and Seizures in a digital world", *Harvard Law Review*, 119 (2006), 531.

[6] Dr Fabio Licata, "The Cybercrime Convention of Council of Europe and Cooperation between Law Enforcement Authorities" (La Convenzione del Consiglio d'Europa sul cybercrime e le forme della cooperazione giudiziaria: una risposta globale alle nuove sfide della criminalità transnazionale), in a workshop of *Consiglio Superiore della Magistratura*, held in Rome on 19 September 2005, at 17, available (in Italian) at http://appinter.csm.it/incontri/relaz/12009.pdf.

[7] On this issue, see point 170 of the *Explanatory Report* on the Convention on Cybercrime: 'Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations'.

[8] A similar approach was adopted by the cybercrime experts who, in 2001, drew up a Model Law on Computer and Computer Related Crime, no. 202, for the implementation of the Convention on Cybercrime in Commonwealth countries (LLM(02)17, October 2002); see section 11 of the 'Model Law' available at http://www.thecommonwealth.org/shared_asp_ files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

[9] John Blau, "Debate rages over German government spyware plan", 5 May 2007, in *Computerworld Security*, available at http://www.computerworld.com/s/article/print/9034459/Debate_rages_over_German_government_spyware_plan?taxonomyName=Security&taxonomyId=17.

[10] For further information on the CIPAV project, see Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', Wired, 18 July 2007, available at http://www.wired.com/politics/law/news/2007/07/fbi_spyware; and Kevin Poulsen, 'Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years', Wired, 16 April 2009, available at http://www.wired.com/threatlevel/2009/04/fbi-spyware-pro/. A similar project developed by FBI was "Carnivore". Carnivore was a system implemented by the Federal Bureau of Investigation that was designed to monitor email and electronic communications. It used a customizable packet sniffer that can monitor all of a target user's Internet traffic. Carnivore was implemented in October 1997 and replaced in 2005 with improved commercial software such as NarusInsight. Talitha Nabbali, *Going for the throat: Carnivore in an ECHELON world - Part II*, *Computer Law and Security Report*, Volume 20, Issue 2, March-April 2004, Pages 84-97. Software of this type has been present in various forms ever since 2001, the year in which the existence of "Magic Lantern" was revealed to the world; this software produced by FBI, NSA and George Lawton, Invasive Software: Who's Inside Your Computer?, Computer, vol. 35, no. 7, pages 15-18, July 2002, doi:10.1109/MC.2002.1016895 (http://utopia.csis.pace.edu/dps/2007/jkile/2005%20-%20Spring/DCS823/Spyware/01016895.pdf). The use of such technology is already widespread and becoming quite a common-currency in the market, making available to (cyber)crime fighting authorities a variety of software solutions. Amongst the many types of software currently available. we can mention, by way of example, the software produced by Web watcher, which is available at the following link: http://www.awarenesstech.com/Law-Enforcement/Remote-Monitoring.html.

[11] Supreme Court of Cassation, 5th Criminal Section, decision no. 16556 of 14 October 2009.

[12] Law on the Protection of the Constitution in North Rhine-Westphalia (Gesetz über den Verfassungsschutz in Nordrhein-Westfalen) as mended on 20 December 2006, articles 5.2(11), 7.1, 5.3, 5.1 and 13 (VSG); Wiebke Abel and Burkhard Schafer, 'The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822', (2009) 6:1 SCRIPTed 106, available at http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp.

[13] Matthew Lewis, "Biologger – A Biometric Keylogger", (IRM Research Paper, December 2008) presented at the Black Hat Conference, Amsterdam, 27-28 March 2008, available at http://www.blackhat.com/presentations/bh-europe-08/Lewis/Whitepaper/bh-eu-08-lewis-WP.pdf; also well as Episode 621 on Internet TV Hak5 entitled "MiTM Javascript Keylogger, Social Engineering Toolkit and more" available at http://www.hak5.org/?s=keylogger&x=0&y=0. This approach

may not be easy to take, because many devices (particularly mobile devices) are protected through the use of DRM; which, in addition to preventing the installation of unauthorized software, provide a level of security that would make it difficult to obtain access by way of Trojan horses or other malicious software.

[14] It is interesting to note that during the proceedings on the constitutionality of the amendment, in addition to three technical experts from academia (Prof. Felix Freiling, Chair of Computer Science at the University of Mannheim, Prof. Andreas Pfitzmann, head of the privacy and security group at Dresden University of Technology and Prof. Ulrich Sieber, director at the Max Planck Institute for Foreign and International Criminal Law) the German Constitutional Court also heard a highly experienced hacker (Andreas Bogk, freelance hacker for Clozure, Inc., and CEO of Chaos Computer Club Events).

[15] Article 10 of the German Basic Law (Grundgesetz): '1. The privacy of correspondence, posts and telecommunications shall be inviolable. 2. Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature'.

[16] Article 13 of the German Basic Law (Grundgesetz): '1. The home is inviolable. 2. Searches may be authorized only by a judge or, when time is of the essence, by other authorities designated by the laws, and may be carried out only in the manner therein prescribed'.

[17] The right 'to informational self-determination' is derived from the combined provisions of article 2.1 and article 1.1 of the German Basic Law (Grundgesetz – GG) which enshrine the rights to 'free development of personality' and to 'human dignity', respectively. The right to informational self-determination was established by the German Constitutional Court for the first time in a historic decision that led up to the passage of the German data protection law (decision of the *Bundesverfassungsgericht* of December 15, 1983, BVerG, paragraphs 65, 1, <43>; 84, 192).

[18] Wiebke Abel and Burkhard Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems" – a case report on BVerfG, NJW 2008, 822'.

Digital Dactyloscopy: A First Design Proposal for a Privacy Preserving Fingerprint Scanning System

Matthias Pocs / Benjamin Stach
Project Group Constitutionally Compatible Technology Design (provet)
Universität Kassel, Germany
{matthias.pocs, benjamin.stach}@uni-kassel.de

Mario Hildebrandt / Stefan Kiltz / Jana Dittmann
Research Group on Multimedia and Security
Otto-von-Guericke University Magdeburg
Magdeburg, Germany
{hildebrandt, kiltz, dittmann}@iti.cs.uni-magdeburg.de

***Abstract*—Biometric technology for crime prevention is emerging. One example is digital contact-less capture of fingerprint traces, which is currently under development. As a first approach we propose the design of a system for securing court evidence. The proposal is based on an evaluation of data formats for the application in future fingerprint scanning systems and is derived from requirements of the German law. Aiming at enhancing privacy, preserving anonymity and protecting against illegitimate "identity change," this proposal shows how to derive technology design proposals from human rights law using a fingerprint scanning system as an example.**

Keywords-privacy and data protection; dactyloscopy; fingerprint scanning system; digital capture; biometric systems; German law on court evidence.

I. INTRODUCTION

Fingerprints are used for decades in forensics to identify that people were present at some point in time at a crime scene or have touched certain items, potentially linking them to a crime. The methods for the acquisition and analysis of traces have not changed significantly over this long period. A major improvement was the introduction of automated fingerprint identification system (AFIS) [1]. This particular system uses an automated identification of potentially matching fingerprints. However, all candidates (usually 15-20) are verified manually by forensic experts. Even with those precautions misidentifications are possible [2].

New acquisition techniques might allow for a non-destructive collection of fingerprint traces with one or multiple sensors in crime prosecution and prevention use-cases [3]. The use of such new techniques can provide more information about a single trace since it can be investigated all over again from different perspectives and using different techniques. This allows for a more thorough investigation by forensic experts and might reduce the risk for misidentifications. However, the application of new sensors and the subsequent investigation of the digitised traces constitute a major change of the generally accepted investigation process of fingerprint traces.

In order to achieve those goals, a first process model for the digital dactyloscopy is introduced in [4]. It is derived from a process model intended for digital forensics because similar precautions must be regarded during the investigation process in digital forensics. The derived process model consists of seven phases: *strategic preparation, physical acquisition, operational preparation, data gathering,* data *investigation, data analysis* and *documentation*. The documentation is divided into a *process accompanying documentation* consisting of a detailed record of all performed actions together with all their parameters, and a *final documentation* as a concluding result of the forensic analysis. Additionally, the security aspects *integrity* and *authenticity* [21] of the processed data must be considered and addressed throughout the entire investigation. Since digital data can be copied and transferred easily, the security aspect of *confidentiality* [21] must be retained to preserve the privacy [20]. Furthermore, the anonymity should be preserved by the unlinkability [20] between a trace and the name until a matching reference sample is found. Subsequently, the security aspects non-repudiation [21], e.g., for the chain of custody, and availability [21] might be required for the investigation of fingerprint traces.

In this paper we evaluate various data formats, including the container format for digitised fingerprint traces from Kiertscher et al. [5], a database-centric approach [6] and a data format for multiple data streams for use in digital forensics [7], for their applicability in a future fingerprint scanning system. For that we derive requirements from the German law. Furthermore, we introduce a legal approach as a foundation for our technical design proposal of a future fingerprint scanning system derived from German law principles. This particular technical design proposal is intended to be applicable for the fingerprint acquisition on crime-scenes and in a forensic lab. It aims at enhancing privacy and preserving anonymity. The standard of data privacy is quite strict in Germany from a comparative law point of view. Therefore, any requirement regarding data privacy might be suited as a showcase requirement. Nonetheless, it has to be considered that criminal law proceedings may differ highly in certain national legislation.

This paper is structured as follows: In Section I, we analyse legal aspects of court evidence. Our legal approach is introduced in Section III. We summarise the process model for the digital dactyloscopy and the forensic data formats that are evaluated in this paper in Section IV. We define main technical requirements and introduce our first design approach in Section V. In Section VI, we analyse the suitability of various selected forensic data formats for future fingerprint scanning systems. Finally, we summarise the challenges for a digitised fingerprint analysis and outline future work in Section VII.

ISBN: 978-1-61208-182-3

II. Evidence in Court

In Germany, statutory law and its judicial interpretation governs court proceedings. Evidence is defined as the assessment of facts (of a case) as an established fact by judicial persuasion. German law recognises several principles in criminal proceedings. The principle regarding evidence is particularly the principle of free evaluation of the evidence, which is set out in § 261 Code of Criminal Proceeding (*Strafprozessordnung*).

Besides, the criminal procedure is a strict *inquisitorial system*. This means the court conducts its own investigation and may not rely solely on the facts and evidence presented by the parties. Furthermore, the *Rechtsstaat* principle (best translated as "law-based state" principle) in art. 20 para. 3 Basic Law (*Grundgesetz*) and art. 6 *European Convention on Human Rights* demands the trial to be conducted fairly. Due to the 'fair trial' principle, police and prosecution have to consider both the burdening and the unburdening facts.

A. Significance of Traces of Fingerprints as Evidence

Fingerprints may be used to identify a person. Every person has an individual fingerprint, even identical twins. Thus, traces of fingerprints are significant as evidence. But it is crucial to point out that fingerprints may only be used to link a certain person to a certain place. Digitalisation might add a greater value to fingerprints as evidence in court.

Digitalisation by contactless devices is a non-destructive method to obtain fingerprints. Until now forensic scientists use so called developer to detect contrasts between the ridge patterns and the surface. The developer is usually a powder or even a chemical reagent. Such technologies destroy any potential DNA traces on the particular fingerprint.

Digitalisation might even produce more information than conventional methods. At the moment, forensic scientists are not able to separate overlapping fingerprints or to estimate the age of a fingerprint. Both may be possible by means of digitalisation and is currently under research.

B. Risks of Digitalisation

Digitalisation might bear several risks. These risks might impede the use of digitised fingerprints in court at all. Thus, these risks need to be excluded by technical means.

1) Tampered Evidence: Digital evidence might be tampered with. The risk of tampering is higher by digital means than by analogous ones. The problem is that manipulations can be done even without special knowledge. Furthermore, manipulation might not be detected at all. This also includes unintentional manipulations, e.g., corruption by storage errors. Tampered evidence would be useless in court because it might not be admissible as evidence at all or would be at worst the cause for an unjust ruling.

2) Evidentiary Value: Digitally collected fingerprints must not be handled differently to normal fingerprints. As an example, a dirt smudge cannot be regarded as a precise imprint only on the basis of being collected digitally and a precise imprint needs to be treated as such. Therefore, the information on the quality of the taken imprint needs to be linked tightly to the presented digital image.

C. Enhancing the evidentiary value

Accordingly, if these risks could be excluded, digitalisation would enhance the evidentiary value of fingerprints as evidence in court. Furthermore, digitalisation might even allow more probative facts to be collected.

1) Secured Chain of Custody: A secured chain of custody can exclude any tampering of the evidence. A complete verification and a complete presentability are necessary for this purpose.

2) Integrated Context Data: Context data can additionally give a description of how the fingerprint has been collected by whom, where and when. Also, the age of the imprint might be added as context data. The forensic scientist needs to add the quality of the found imprint. This ensures that all the collected data is bound together. The context data needs to be presentable.

3) Conclusion: For the purpose of evidence, any data of the digitised fingerprint has to be stored in a secured chain of custody. This involves any additional context data, such as location and time of collection or age as well as quality of the imprint. Any context data would enhance the evidentiary value contrary to plain analogous forensic scientists' transcript by including it into the secured chain of custody.

III. Legal Framework

The German constitutional principle of the *Rechtsstaat* lays down that innocence of persons accused of a crime be assumed until evidence is furnished [8]; this is also enshrined in art. 6 *European Convention on Human Rights*. In relation to data processing one has to comply with the fundamental right to informational self-determination according to art. 2 para. 1 i.c.w. art. 1 para. 1 *Grundgesetz*. This aims at enhancing privacy and preserving anonymity of nonsuspects and protecting them against "identity change."

A. Legal Requirements

Currently fingerprints at crime scenes are manually collected by the police officer in charge of securing evidence. During criminal proceedings the fingerprint as well as the officer's record about securing the fingerprint with his/her signature on that record are furnished as documentary evidence pursuant to §§ 249 ff. *Strafprozessordnung*. The authenticity of the record is proven by means of the officer's testimony to the signature on the record pursuant to §§ 48 ff. *Strafprozessordnung*. For automatic capture of fingerprint traces, this means that it needs to have a solid scientific and technological basis, be applied without error and ensure that the fingerprint traces have a quality suitable for furnishing evidence [9]. Moreover, integrating context data can increase the evidentiary value.

B. Legal Criteria

There are several legal criteria that specify the general legal criteria of scientific and technological basis, error-free application, trace quality and integration of context data.

For establishing the existence of a scientific and technological basis we may put forward several criteria (testing, standards, comprehensibility by experts/judges, and error rates). Concerning the error rates one has to consider that the fingerprint scanning system does not decide whether or not a fingerprint belongs to a certain person but only digitises the trace of a fingerprint. Deciding on similarity of two fingerprints is not part of it. Nonetheless, there may be errors (wrong choice of surface material, "regions-of-interest," or distinction surface/fingerprint). The significance or the error rate needs to be explored in the future.

Concerning the error-free application of the method the fingerprint scanning system offers an opportunity. This is due to the fact that the fingerprint captures are automated and the method can be applied without error as far as it is automated. One can clarify what processes are automated.

Avoiding error or manipulation is achieved by measures of data security relying on the state of the art [10]. All stages of processing within the scanning system are logged in a secure way [11]. These processes also comprise manual inputs of additional information that is necessary for the evaluation of secured fingerprints. The data must be secured from the time of data capture.

Sophisticated encryption oriented towards the state of the art and secure access should be used [12] [13]. Further the scanning system may be protected using digital watermarks. Watermarks can be reversible or irreversible. As long as the data are not devaluated in a way that the scientific basis does not apply anymore, irreversible watermarks are preferable because they guarantee increased data integrity.

The trace quality relies on the trace and properties of the surface material, which has to be considered when designing the system. One can explore how to collect information about the trace quality by automatic means; this may be a research question for the future. Surface material information is manually entered; also with conventional methods such information needs to be collected [14]. However, it needs to be adapted and defined for the scanning system.

Integrating context data is a new possibility the scanning system offers. Currently the police officer is in charge of proving the time of securing the evidence and place of the crime scene using his/her respective record. With the fingerprint system, the information about time and place could be captured automatically (secured system time/GPS or time/place stamps) in order to rule out confusion of different investigations. In this way the evidentiary value of the captured fingerprint data is increased.

In addition, research promises to determine additional context information about the fingerprint. First the scanning system can determine the age of the fingerprint. The age of such traces is decisive to establish whether or not the trace was left during the criminal activity [15]. Furthermore, the system can separate overlapping fingerprints. Moreover, spoofing the capture device by using artificial fingerprints can be revealed. Such attacks will be more likely in the future if use of biometric systems will increase [16].

IV. State of the Art

We use the process model for the digital dactyloscopy [4] to describe our concept of a criminal court proved design of a future non-destructive optical fingerprint scanning system. Furthermore, we analyse different data storage formats or concepts as a base for the digitised forensic investigation.

A. Process model for the digital dactyloscopy

The process model for the digital dactyloscopy [4] consists of seven phases. During the first phase *strategic preparation* (SP) potential investigations are prepared. This phase describes procedures and techniques used ahead of a specific incident. Those include the acquisition and installation of sensors, as well as training arrangements for the personnel. Furthermore, a software directory, sample material and aging models should be created and evaluated by benchmarking [17]. Subsequently, guidelines for the physical acquisition should be defined for crime scene investigators to avoid any alteration of fingerprint traces.

The *physical acquisition* (PA) describes the identification and acquisition (e.g., seizure) of physical objects that might contain fingerprint traces. The crime scene investigator should also decide whether the object can be transported to a forensic lab for the acquisition or whether it is better to acquire it directly on the crime scene (e.g., if the object is too large or if the trace might be destroyed during the transport).

The *operational preparation (OP)* describes all processes that are required prior to the digital acquisition. In particular, it includes the choice of the appropriate acquisition sensors and processing methods to achieve the highest possible quality of the digitised trace. Here the results of the strategic preparation will be used.

During the *data gathering* (DG) several actions are performed to acquire the fingerprint traces from a particular object using contact-less sensory equipment. Firstly, the required acquisition parameters and material properties are determined. Secondly, a coarse scan is performed to detect Regions-of-Interest (ROI) that need to be acquired with a detailed scan. Subsequently, each ROI is acquired using high-resolution detailed scans.

The *data investigation* (DI) contains all pre-processing steps prior to the fingerprint ridge pattern analysis. In this phase overlapping fingerprint patterns are separated, the age of each pattern is determined and the visibility of the ridge pattern is enhanced for the manual analysis using pre-processing techniques.

The identification of the fingerprints is performed during the *data analysis (DA)*. It is performed manually with optional machine assistance (e.g., feature extraction and highlighting). The investigation should strictly adhere to current investigation standards: the analysis, comparison, evaluation, and verification (ACE-V) methodology, etc. [1]

Subsequently, the results are summarised in the phase of the *documentation (DO)*. Besides the concluding final documentation a process accompanying documentation contains a detailed log of all performed investigation steps throughout the whole process. This allows for an enhanced comprehensibility of the course of the investigation.

B. Forensic data storage and exchange formats

Various formats for the storage and exchange of forensic traces exist. In this paper we compare the *data format for the interchange of fingerprint, facial & SMT information*

(ANSI/NIST-ITL 1-2000) [18], the *Advanced Forensics Format (AFF4)* [7], a container format for digitised fingerprint traces [5] and a database centric approach for digitised fingerprint traces [6].

The *data format for the interchange of fingerprint, facial & SMT information* (ANSI/NIST-ITL 1-2000) is used for the exchange of fingerprint data for the automated fingerprint identification systems (AFIS) [1]. The design goals for this particular format are *openness*, *non-intrusiveness*, *inter-operability* and *wide usage*. The data format consists of ASCII and Binary data records. Those logical records include transaction information, user-defined descriptive texts, fingerprint images in different resolutions and encodings (e.g., Binary and greyscale), a user defined image, an image of the handwritten signature of the subject and/or the officer, minutiae data, images of latent prints or Common Biometric Exchange Formats Framework (CBEFF) [19] [19] Biometric data records. It supports various image formats for the fingerprint image: uncompressed images, WSQ version 2.0, lossy and lossless JPEG, lossy and lossless JPEG 2000 and PNG. Images can be binary, greyscale or colour data.

The *Advanced Forensics Format 4 (AFF4)* [7] is designed for digital forensics. It is able to store multiple digital traces within a single volume. The data can be stored as a *directory volume* or *Zip64 volume*. Both, digital traces and meta-data can be stored within this structure. A directory volume is a directory on the file system of a computer, which contains the segments of the volume named after a unique Uniform Resource Name (URN). A Zip64 volume contains a Central Directory at the end of the archive, which consists of a list of pointers to each digital trace within the volume. The format natively supports digital signatures to fulfil the security aspects *integrity* and *authenticity*. The *confidentiality* of the stored data can be preserved using an integrated stream based encryption scheme, which supports different access levels. Furthermore, AFF4 is designed to support distributed evidence.

A very similar data format, especially for the digital dactyloscopy, is introduced by Kiertscher et al. in [5]. It has a directory and a zip-file operation mode, too. In contrast to AFF4 it contains a tree of editions that can form a simple chain-of-custody to comprehend or audit the investigation process. It includes a hierarchical hash tree based on digital signatures to ensure *integrity* and *authenticity* for the data within the container. The underlying model supports encryption for the digitised traces and a portion of the meta-data. However, all encrypted data must be decrypted prior to any transformation of the container.

The database-centric approach of the *Fingerprint Verification Database (FiVe DB)* [6] has several advantages and disadvantages compared to the file based data exchange formats. It uses a watermarking approach for the digitised traces. The compression and difference expansion based watermark is embedded within the areas of the data, which contain the fingerprint. Those areas are compressed to gain storage for the meta-data. The embedded data is divided into a public and a private (encrypted) part. The latter contains the original fingerprint impression to ensure privacy. The embedded data contains digital signatures to ensure authenticity and integrity. The required location map for embedding areas is embedded throughout all data using a difference expansion approach. The hybrid database approach [6] employs user-defined functions to insert and read digitised traces. Those functions verify the authenticity and integrity of the transferred and stored data. Furthermore, it is easily possible to log any access to the data to create a chain-of-custody. However, *FiVe DB* requires a direct connection to the database to transfer the data. Alternatively, the watermark protected digitised traces can be exchanged as files, which enables a verification of the *authenticity* and *integrity* and ensures the *confidentiality* by the encryption of the private data. However, without the database the chain-of-custody information are quite limited within the watermark, due to the limited embedding capacity.

V. Technical Design Proposal

In this paper we focus on the challenges of the digitisation of the investigation of fingerprint traces. Our technical design proposal is derived from the process model for the digital dactyloscopy ([4], see Section IV.A). In contrast to the process model we primarily regard the transfer of digitised fingerprint traces (Figure 1).

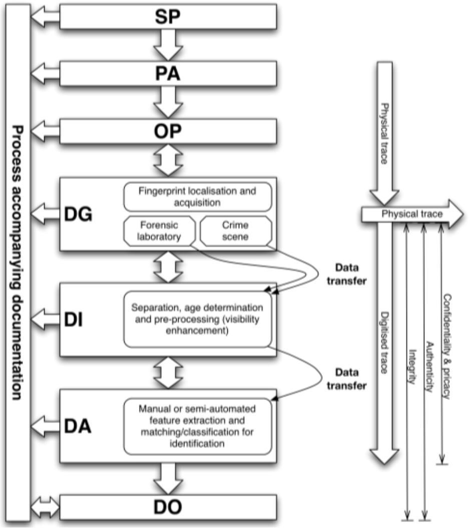
SP
PA
OP
DG
Fingerprint localisation and acquisition
Forensic laboratory
Crime scene
DI
Separation, age determination and pre-processing (visibility enhancement)
DA
Manual or semi-automated feature extraction and matching/classification for identification
DO
Process accompanying documentation
Data transfer
Data transfer
Physical trace
Physical trace
Digitised trace
Integrity
Authenticity
Confidentiality & pricacy

Figure 1. Our technical design proposal for a fingerprint scanning and analysis system.

The technical design has to cover two possible use-cases: *on crime scene trace acquisition* and the *acquisition in a forensic lab*. Since we focus on the newly digitised part of the forensic investigation, mostly the phases of *data gathering (DG), data investigation (DI)* and *data analysis (DA)* are relevant including the data transfer between the phases. The technical design of a fingerprint scanning system must address the security aspects of *integrity* and *authenticity* for the gathered and processed data to be able to detect any modification (see Section IV.B). Thus, the final documentation should contain enough data to verify the integrity and authenticity of the data throughout the investigation process. Furthermore, it might be necessary to address the confidentiality of the acquired data to preserve privacy (see

Section III). This is especially needed if the digital traces are transferred. A criminal court proven design requires a detailed chain-of-custody for both, the digitised trace and the physical object containing the trace (see Section II.C.1).

With the data gathering (DG) the digitised trace is acquired. It is very important to retain a link between the physical object and its digital pendant or pendants. Therefore, multiple additional information, or meta-data, must be recorded. Such data includes various information, e.g., who acquires the trace, where is the trace acquired (especially for an on crime scene acquisition), when is it acquired, how are the environmental conditions during the acquisition or for which case are the traces acquired.

Afterwards, the collected data is transferred for a detailed investigation. This might include the transfer over insecure channels, e.g., if the data is send directly from a crime scene to a forensic investigation agency. It is crucial, that no data is altered or leaked during the transfer to preserve the evidentiary value and the confidentiality also as a pre-requisite for privacy. In the following *data investigation* the traces are prepared for the manual analysis.

During the *data investigation (DI)* the age of a fingerprint might be determined, overlapping fingerprints might be separated and the visual image of the ridge pattern might be enhanced for a better visibility of features during the analysis. However, at least the separation and the visibility enhancement involve an alteration of the original data. Thus, all parameters how the data is altered must be recorded and the original data must be accessible, too.

After the data investigation, the data are transferred to dactyloscopic experts for the extraction of biometric features and the subsequent identification of the fingerprint trace. In this *data analysis (DA)* phase additional data transfers might be necessary: transfer of the data to other forensic investigation agencies for the verification of the results (see ACE-V methodology [1]) or the transfer of the data for the comparison with AFIS databases (see [1]). The authenticity, integrity and confidentiality of the transferred data and the whole transfer process must be ensured because it might include insecure communication channels.

If a particular trace is identified a final documentation is created. Similar to the ACE-V methodology [1], this concluding result of the investigation should contain all investigation results. The digitised trace itself should not be included in the report. Thus, it is not required to ensure the confidentiality of the data because it does not contain any biometric traits. The integrity and authenticity of the documentation must be ensured in a digital representation.

Furthermore, the entire process needs to be documented within the process accompanying documentation.

In the following section, we exemplarily evaluate data formats according to their suitability for a future fingerprint scanning and analysis system. For that we derive the following technical requirements from our design proposal:

1. Authenticity protection,
2. Integrity protection,
3. Confidentiality/privacy protection,
4. Ability to store multiple traces and intermediate results of the investigation,
5. Ability to store various meta-data.

The requirement of a chain-of-custody can be fulfilled if the format supports all of the technical requirements except the confidentiality protection. The process accompanying documentation, e.g., from secure logging facilities, should be stored as meta-data within the file format.

VI. Analysis of forensic data formats

In this section, we analyse data formats towards their suitability for a future latent fingerprint scanning system. The *data format for the interchange of fingerprint, facial & SMT information* (ANSI/NIST-ITL 1-2000) [18] is already used in forensic investigations for the data exchange between different AFIS databases. Hence, it could be seen as generally accepted and should fulfil the legal requirements (Section III.A). However, this format does not support any techniques to preserve the privacy or confidentiality of the transferred data. Moreover, it does not preserve the integrity or the authenticity of the transferred data. Only a digital image of the signature of the acquisition officer is included within the file. The format supports multiple samples of different biometric traits and user-defined meta-data. Thus, at least the technical requirements 4 and 5 from our technical design proposal in Section V are addressed.

The *Advanced Forensics Format (AFF4)* [7] is not designed for the forensic analysis of biometric traits. However, it has several advantageous features for digitised forensics. The security aspects integrity, authenticity and confidentiality are sufficiently addressed by the data format if activated by the user or the used software. Furthermore, multiple traces or intermediate results and meta-data can be stored in this file format, fulfilling our technical requirements for a future fingerprint scanning system. Moreover, the ability to access data remotely through encrypted streams and the embedded access restriction enables a distributed investigation while preserving the confidentiality as a prerequisite for privacy. Additionally, different traces on the same object can be stored within a single trace file as a digital representation of the physical evidence bag.

The container for the digital dactyloscopy [5] ensures the integrity, authenticity and, optionally, confidentiality of the stored data, too. It enables the storage of multiple traces and intermediate results within the container file. Additionally, meta-data can be stored within separate files in the container. Thus, the container format fulfils our technical requirements for a future fingerprint scanning system, too. However, if the concurrent access to different traces within the container is necessary it is required to clone the container, which requires a merging-strategy if the two containers are joined again.

The database-centric approach *FiVe DB* [6] significantly differs from the file based approaches. The processed image files fulfil our technical requirements *integrity*, *authenticity* and *confidentiality* by the embedded watermark. A limited amount of meta-data can be stored directly within the image file. However, it is not possible to store multiple traces or intermediate results within a single image. The advantage of this approach is the superior access restriction and automated logging facilities of the database management system. The disadvantage is the limited support for a data exchange without direct access to the database.

Table 1 summarises our evaluation for the data formats.

TABLE I. SUMMARY OF OUR EVALUATION RESULTS FOR THE STORAGE AND TRANSFER OF DIGITISED TRACES (+ REQUIREMENT FULFILLED; - REQUIREMENT NOT FULFILLED)

Technical requirement Storage / transfer	**ANSI/NIST-ITL 1-2000**	**Advanced Forensics Format (AFF4)**	**Container for the digital dactyloscopy**	**FiVe DB**
Authenticity protection	-/-	+/+	+/+	+/+
Integrity protection	-/-	+/+	+/+	+/+
Confidentiality protection	-/-	+/+	+/+	+/+
Multiple traces / intermediate results	+/+	+/+	+/+	+/-
Meta-data	+/+	+/+	+/+	+/+

In conclusion, the current ANSI/NIST-ITL 1-2000 is insufficient for a future fingerprint scanning system due to the lack of any addressed security aspects. In general, the other formats in this exemplary evaluation are appropriate.

VII. CONCLUSION AND FUTURE WORK

In this paper we proposed a criminal court proved design for a new fingerprint scanning system. For that, we analysed current legal requirements and derived a new legal approach. We use this framework to introduce a potential design for a digitised latent fingerprint acquisition and analysis system. It aims at enhancing privacy and preserving anonymity. We preliminarily modelled the data flow and data transfer.

Subsequently, we derived technical requirements for data formats using the technical design proposal and the legal approach. Our exemplary analysis of data formats using our requirements indicates that the currently used ANSI/NIST-ITL 1-2000 format is insufficient especially regarding the security aspects integrity, authenticity and confidentiality and thus unsuitable for privacy preserving transfers over insecure communication channels. The other data formats are appropriate for a future fingerprint scanning system.

In future work different sensors and processing techniques should be evaluated towards their applicability in a fingerprint scanning system. Furthermore, the necessary amount of meta-data for the chain-of-custody should be analysed to fulfil the requirements of criminal courts. This might improve the evidentiary value of each trace, too.

ACKNOWLEDGMENT

The work in this paper has been funded in part by the German Federal Ministry of Education and Science (BMBF) through the Research Programme under Contract No. FKZ: 13N10820 and FKZ: 13N10818.

REFERENCES

[1] Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST), "The Fingerprint Sourcebook," NCJ 225320, 2011.

[2] S. A. Cole, "More than Zero: Accounting for Error in Latent Fingerprint Identification," Journal of Criminal Law and Criminology, Vol. 95, No. 3, pp. 985-1078, 2005.

[3] M. Hildebrandt, J. Dittmann, M. Pocs, M. Ulrich, R. Merkel, and T. Fries, "Privacy Preserving Challenges: New Design Aspects for Latent Fingerprint Detection Systems with Contact-Less Sensors for Future Preventive Applications in Airport Luggage Handling," in: Biometrics and ID Management, LNCS 6583, pp. 286-298, 2011.

[4] M. Hildebrandt, S. Kiltz, I. Grossmann, and C. Vielhauer, "Convergence of Digital and Traditional Forensic Disciplines: A First Exemplary Study for Digital Dactyloscopy," in Proceedings of the thirteenth ACM multimedia workshop on Multimedia and security (MM&Sec '11), pp. 1-8, 2011.

[5] T. Kiertscher, C. Vielhauer, and M. Leich, "Automated Forensic Fingerprint Analysis: A Novel Generic Process Model and Container Format," in: Biometrics and ID Management, LNCS 6583, pp. 262-273, 2011.

[6] M. Schäler, S. Schulze, R. Merkel, G. Saake, and J. Dittmann, "Reliable Provenance Information for Multimedia Data Using Invertible Fragile Watermarks," In 28th British National Conference on Databases (BNCOD), LNCS 7051, pp. 3-17, 2011.

[7] M. Cohen, B. Schatz, and S. Garfinkel, "Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow," in Digital Investigation, 6(Supplement), pp. 57-68, 2009.

[8] BVerfGE (Bundesverfassungsgerichtsentscheidungen, respectively, collection of decisions of the Federal Constitutional Court of Germany) 110, 1 (22 f.), 1996; 82, 106 (118 ff.); 74, 358 (369 ff.); 35, 311 (320); 19, 342 (347 f.).

[9] B. Kasper, “Freie Beweiswürdigung und moderne Kriminaltechnik,” Hamburg 1975, p. 119.

[10] For data security BVerfGE 125, 260 (para. 224), 2010; also § 17 para. 1 subpara. 2 Data Protection Directive 95/46/EC.

[11] A constitutional safeguard according to BVerfGE 125, 260 (224).

[12] In detail A. Roßnagel and P. Schmücker, “Beweiskräftige elektronische Archivierung - Bieten elektronische Signaturen Rechtssicherheit?,” Bonn2006, pp. 13 ff.

[13] M. Knopp, “Digitalfotos als Beweismittel,” in Zeitschrift für Rechtspolitik, 2008, 156 w. f. r.

[14] S. Tietze and K. Witthuhn, “Papillarleistenstruktur der menschlichen Handinnenfläche (Band 9),” Luchterhand, 2001, p. 76.

[15] Bundesgerichtshof, decision of 25.09.2007 – (4 StR 348/07).

[16] Pfitzmann, A., Informatik-Spektrum 10/2006, p. 353.

[17] S. Kiltz, M. Leich, J. Dittmann, C. Vielhauer, and M. Ulrich, ”Revised benchmarking of contact-less fingerprint scanners for forensic fingerprint detection: challenges and results for chromatic white light scanners (CWL)”, Proc. SPIE 7881, 78810G, 2011.

[18] The INTERPOL AFIS Expert Group, “Data format for the Interchange of Fingerprint, Facial & SMT information”, INTERPOL Implementation Version 5.03 (ANSI/NIST-ITL 1-2000), [Online]. Available: https://www.interpol.int/Public/Forensic/fingerprints/RefDoc/ImplementationV5.pdf, 2011 [last checked 19.11.2011]

[19] National Institute of Standards and Technology, “CBEFF Common Biometric Exchange Formats Framework”, NISTIR 6529-A, [Online]. Available: http://csrc.nist.gov/publications/nistir/NISTIR6529A.pdf, 2004 [last checked 19.11.2011]

[20] A. Pfitzmann, and M. Hansen, “A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management”, v0.34, [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, 2010 [last checked 22.11.2011]

[21] S. Kiltz, A. Lang, and J. Dittmann, „Taxonomy for Computer Security Incidents“, Cyber Warfare and Cyber Terrorism, pp. 412-417, ISBN 978-1-59140-991-5, 2007.

ISBN: 978-1-61208-182-3