

Biometrics

March 8

2009

---

By Jonathan Auer, Matthew Buckle, Anton Li

Group 4

---

## **Background Information**

Biometrics is a fast growing field that is very controversial. Identity and privacy issues are the main reasons why many civil groups and individuals oppose it. Face recognition biometrics is not as widely available as fingerprint scans, but with constant technological changes, researchers will improve this security technology for the twenty-first century. Implementing biometric technologies as a preventive measure against terrorism is not only a concern in Germany, but also within the international community.

In the recent wake of the terrorist attacks, many countries have considered introducing new safety measures such as ID cards that include biometric identifiers such as fingerprints, facial recognition, and iris scans. In the U.K., Canada, and the U.S., the debate over implementing the new biometric technology has mostly focused on the cost issues. According to a human rights group, Privacy International, “articulations of ‘asylum seekers’ and ‘immigration control,’ ‘benefits fraud,’ and ‘terrorists’ from government were often countered with articulations of ‘risks,’ ‘costs,’ and ‘centralized databases’ from civil society organizations.”

On 17 October 2000 the European Council approved a resolution introducing minimum security standards for passports. The Thessaloniki European Council on 19 and 20 June 2003 confirmed the need to take common measures on biometric identifiers and data for documents for third-country nationals, European Union citizens’ passports and information systems. On 12 December 2003 the EU Council invited "the Commission to submit in due time a proposal for the introduction of biometric identifiers in passports" (the Activities of the EU, pars. 10-12). In addition, the introduction of biometric passports shows that the Member States that are participating in the United States Visa Waiver Program need to align themselves with the

relevant US legislation so that their citizens can enter US territory without a visa. The Thessaloniki European Council concluded that there is a need for a systematic approach to the introduction of biometrics into visas, residence permits and passports (the Activities of the EU, par. 13).

The recommendations for passports, visas, and residence permits include two mandatory biometric identifiers: the facial image and fingerprints. The facial image has been chosen as a mandatory biometric identifier for passports. Fingerprint scans can be added as an extra biometric identifier at the discretion of the EU Member States. The proposal will be considered by the EU Council and the European Parliament (Rapid-Press Release, par. 1).

The aim of the Commission proposal is to upgrade the security features adopted by the Council in October 2000 in its resolution on minimum-security standards for passports and other travel documents. It will also render these features legally binding. The proposal will therefore set a harmonized high security standard for passports within the European Union of 25 Member States. Just as was the case in the resolution, the Commission sets out the minimum standards and will not stop Member States that wish to go further.

In 2005 Germany became the first European Union country to introduce biometric passports. The European Union requires its member states to begin issuing biometric passports by August 2006 (Rapid-Press Release, par. 6). German passports have a smartcard chip and loop antenna embedded into the front cover page. The chip and antenna are not easily visually recognizable, but their presence is indicated using the International Civil Aviation Organization (ICAO) biometric passport symbol at the bottom of the front cover. It carries all the data printed in the passport, including a JPEG file of the photo, protected by a digital signature. As of 1

December 2007, two fingerprint scans are added to the chip (The Federal Ministry of the Interior, par. 5).



Biometric registration in Germany will not be available to everyone. It will be limited to citizens of certain countries, including some "high-risk" countries that German authorities suspect of harboring potential terrorists. It is not clear which countries will be affected by this new rule. The introduction of the biometric identification procedures is based on the "Law on Combating Terrorism" that took effect in January 2002, indicating security concerns in the wake of the 9/11 terrorist attacks in the U.S. (Oezcan, pars. 3-4).

An additional benefit of biometric identifiers, from the perspective of German officials, is its possible usefulness regarding requests to deport failed asylum seekers. Under international law, Germany cannot deport individuals without knowing their country of origin. Some countries, from which Germany's asylum seekers originate, have in the past used uncertainty about the background of failed asylum seekers to support a refusal to take back their citizens. The new biometric measures may make it harder for asylum seekers to hide their country of origin, therefore making them easier to deport following failed bids for asylum (Oezcan, pars. 5).

## **Societal Implications**

In 2002, the new Anti – Terrorism law was passed in Germany. According to Dirk Haubrich in his article “September 11, Anti-Terror Laws and Civil Liberties: Britain, France and Germany Compared,”, laws of this nature curtailed civil liberties in eight different areas, although he does not specify what those areas are (Haubrich). The 2002 Anti – Terrorism law mandates three criteria when authorities are considering admitting asylum seekers or visa applicants to Germany. The first criterion is that the individual has not threatened the constitutional values of democracy. The individual must also not have a history of resorting to violence in order to further his or her political goals, and finally must not have participated in or be involved with a group supporting international terrorism. However, the mandates of the Anti – Terrorism law, especially the language they use, can be considered vague as the terms of terrorist and terrorism have not been specifically defined. This is the opinion of many writing on the subject of terrorism and laws attempting to protect the citizenry of a nation or state, particularly Germany. As terrorism becomes more and more a part of the policy and legislation of the government of Germany, technologies to aid these policies and laws will become more prevalent. The ePass, implemented by German authorities in 2005 is just one step in the digitalization of border control and personal identification. However, questions of further electronic measures worry some, especially in regards to the social impact biometrics may have.

Julian Ashbourn, who is the chairman of the International Biometric Foundation and the creator of the AVANTI non – profit online biometric resource, authored a report for the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs of the European

Parliament (LIBE). This report outlined the impacts biometrics could have on society as well as the different groups affected by the specified technology. Ashbourn was one among three other experts on the topic of biometrics and society. His article in particular, “The Social Implications of the Wide Scale Implementation of Biometrics and Related Technologies,” argues that these technologies will mostly have a negative impact on the way society operates and also the way in which governments relate to individuals ([www.europeanbiometrics.info](http://www.europeanbiometrics.info)). The author points out that while Germany’s government and other governments cite the need for biometrics to track known and suspected terrorists, biometrics and the laws associated with it could allow these governments to exercise “stringent controls” over citizens for their “protection.” Ashbourn explains that this could be done through a variety of national identity schemes (although he does not specify what these schemes would be), as well as border control programs. He also argues that there is a problem with governments assuming that acts of terrorism come from abroad, therefore he questions the need for the border control programs previously mentioned. Ashbourn states that “blurring of citizen entitlement” such as crossing borders as well as access to public services is a major problem for a number of reasons. First, governments are increasingly taking and sharing sensitive personal data from individuals without their permission or knowledge. Further, it is not clear what happens to this data, how long it is stored, or who is allowed to view or use the data during this period of time. Widespread implementation of biometrics also concern Ashbourn because governments in countries like Germany and the United States have started profiling and making assumptions about individuals based on data such as family name, ethnicity, and/or travel history. This could lead to discrimination or the denial of important public services. More distressing to Ashbourn are recent polls that have been taken showing that

the ordinary citizen is more distrustful of government than in previous years. He states that this could lead to extremism if government continues its current actions.

This is a worrying trend as it potentially provides a breeding ground for extremist views to develop, as all history shows us. It follows then, that we must be extremely careful when introducing technologies into the public sector which may be viewed as 'big brother' enablers. Adding a biometric identity check to everyday transactions may, depending upon how it is orchestrated, promote just such a view [ . . . ] it is becoming clear that government agencies in general are inclined to take advantage of the perceived terrorist threat in order to introduce a variety of schemes under the general banner of 'security', whose real agenda is quite different.

While this may be the opinion of someone who fears an Orwellian style world, Ashbourn's views do carry some weight and merit.

Ashbourn's opinions on biometrics aside, investigation into the public realm of biometrics, as well as the concern for privacy should be made. Many argue that biometrics could streamline transactions on a governmental basis as well as a commercial one. Imagine being able to go to a retail location and simply scanning your fingerprint in order to make a purchase. At this point the money is deducted from your account and the hassle of writing a check, paying with cash, or using a debit or credit card is negated. On the other hand, with all of the information that is linked to your fingerprint, companies could share information with each other and could subject the consumer to unyielding advertisements. This brings up the issue of the privacy of individuals in Germany and abroad. Propositions have been made to eventually put microchips under the skin or in the fabric of clothing to further streamline a multitude of transactions. This type of biometric technology could provide assistance to rescuers searching for victims and survivors of disasters, for example. However, individuals could also lose their anonymity in relation to their freedom of movement. Ashbourn would argue that something of this nature would put law-abiding citizens into the same spot as criminals or persons with a criminal record.

The growing issue of terrorism among governments has increased the market for biometrics. This technology has sparked discussion in the international community over the implementation of high tech measures. While some argue that biometrics are too costly and infringe on personal liberties such as privacy and anonymity, others dispute that this technology is an important and necessary measure, and that no cost is too great in the name of security. Nevertheless, many countries have gone forward with the introduction of biometric technologies, not only because of the requirements sanctioned by the United States, but also because of their own need for security and protection against terrorist acts.

### **Business and Financial Costs**

Requirements for greater security in Germany and the European Union are driven by many factors including the safety and protection of the people. The introduction of the “Patriot Act” required all passports for visitors who are citizens of the so-called “visa waiver countries” to the USA to be upgraded to contain biometric identifiers. This requirement has resulted in conflicting responses among those who want biometrics as an added security feature and those who are skeptical about the safety features and possible dangers of biometrics. The introduction of an E-passport following the September 11 attacks in the United States is a difficult and controversial issue among many Germans.

The development and use of an identity solution requires a secure design, including advanced software, control and security. The biometric data and personal details on passports will be stored on national and EU-wide databases and be accessible through the Visa Information system called “VIS” held on the Schengen Information systems “SIS II.”

The financial model found in the essay “The Price of Convenience,” used to describe the economics and financial decisions behind the development of biometrics is the Price of



Convenience (POC) model. The Price of Convenience model (POC) attempts to balance price (P), in terms of perceived loss of privacy, against the conveniences (C) of adoption, and perceived impact on collective security (S).

The (POC) model presents a basic financial model to understand the interaction at three different levels: primary, secondary, and consequences. Primary includes the three main groups involved in producing a biometrics program: government, companies, and industry groups. Secondary includes the important role of the media in convincing the public to adopt biometrics for safety and security reasons and to prevent any assimilation issues that could rise. The last level is a combination of the primary and secondary levels. Consequences attempts to recognize the issues presented in the two previous levels, with the goal of visualizing change and the gradual adoption of biometrics, according to Unisys website (<[http://www.uni-koblenz.de/~iwi/publications/ag-hampe/NgkSwaHamReb\\_2005\\_Biometrics\\_COLLECTeR-Europe.pdf](http://www.uni-koblenz.de/~iwi/publications/ag-hampe/NgkSwaHamReb_2005_Biometrics_COLLECTeR-Europe.pdf)>).

According to the “European Biometrics Portal,” the LSE e-ID (London school of Economics) alternative blueprint for an ID card with biometrics features rivals with the Home Office’s design to gain the rights to produce the electronic ID card. Home Office announced that the LSE’s costing analysis of the government’s ID proposal “includes a number of inaccurate assumptions that has inflated their cost estimates.” The LSE e-ID report claimed that the true costs of the government’s proposed e-ID scheme would be several times higher than the figures estimated by the Home Office.

In June 2005, the LSE published a report entitled “The Identity Project: An Assessment of the UK Identity Cards Bill and Its Implications” which was written by fourteen professors, was based on a six month study and involved extensive consultations with nearly 100 industry

representatives, experts and researchers from the UK and around the world. The report concluded that an ID card system could offer some basic public interest and benefits for the commercial sector. However, it also identified many areas of concern with the government plans, including unclear purposes, technological problems, legal and privacy issues, security risks, citizens' acceptance, burden for businesses, and extremely high up front costs. The report also proposed an alternative ID card scheme that would still incorporate biometrics, but would be simpler and cheaper to implement while giving citizens more control over who can access data about them.

A low estimate of the Home Office's cost and benefit figures revealed in the "European Biometrics Portal," shows that the proposed ID registration system requires fourteen or more years to show a positive net return on investment. With a less favorable independent cost, it estimated that the scheme is never likely to break even. The Home Office figures also suggest that the private sector should carry the majority of the program's costs and risks since close to two thirds of the benefits lie in this sector. Finally, removing the more controversial aspects of the system such as the National Identity Register could produce substantial cost savings while still delivering close to 90% of the identified benefits.

Currently about 100 German companies employing thousands of people produce biometrical products or deal with the system integration of Biometrics. Most of these companies are located in Bavaria and Baden-Württemberg, followed by Hessen, North Rhine-Westphalia and Berlin. The technology behind Biometrics will give many people in Germany profitable jobs for years to come. The market for biometrical technologies is strongly affected by political decisions: Soreon Research estimates that the government will account for 45% of the total German demand by the year 2009. These figures were found on the Just 4 Business website at

<http://www.just4business.eu/2007/10/biometrics-market-offers-huge-opportunities-to-companies/>.

According to information found on the Cross Match website, some of the companies involved in the Biometrics sector include: Cross Match Technologies, Securstar GmbH, Lufthansa Systems Group GmbH, and Bundesdruckerei GmbH. Cross Match Technologies, Inc. is a leading global provider of high-quality biometric identity management solutions used to capture and process the unique physiological characteristics of individuals to establish and verify their identities. Cross Match's government and commercial customers use its biometrics solutions in a variety of security and surveillance programs for protecting people, property and privacy. Securstar GmbH is a German company offering biometric fingerprint and smartcard readers. Smartcard readers are a component found in the E-ID cards and passports used in Germany.

In October 2005, IDG News Service reported that two German companies developed a new biometric system for identifying airline passengers during the boarding process. Lufthansa Systems Group GmbH, the IT sector of German airline Lufthansa AG, and high-security document producer Bundesdruckerei GmbH are demonstrated their jointly developed SecBoard system at the InterAirport trade show in Munich at the end of October. The system is designed to conduct biometric checks on passengers prior to boarding an aircraft. This will play a significant role in the introduction of "trusted passenger" programs planned by the airline industry to increase security. Passengers with an electronically readable identity card containing biometric data will also benefit from the technology. Both companies said the biometrics ID cards will allow passengers to move more quickly through the airport than passengers without ID cards.

## **Conclusion**

The growing concern governments have with terrorism has increased the market for biometrics. This technology has sparked discussion in the international community over the implementation of such high tech measures. While some argue that biometrics are too costly, infringe on personal liberties such as privacy and anonymity, others dispute that this technology is an important and necessary measure, and that no cost is too great in the name of security. Nevertheless, many countries have gone forward with the introduction of biometric technologies, not only because of the requirements sanctioned by the United States, but also because of their own need for security and protection against terrorist acts.

Germany is leading the way in implementing the new biometric technologies in Europe. It was the first European Union country to introduce the biometric passport. In March 2008 it became the first European Union country to sign a bilateral agreement with the United States to share access to national criminal databases (Bain, par. 1). While this agreement may become a model for other states to follow towards creating an international biometric database, it also raises many concerns over the data privacy.

Based on our research, it seems that the future of biometrics holds great potential not only for law enforcement applications but for private industry uses as well. As of today, we believe the benefits of using biometrics outweigh the negative aspects. However, biometric technologies still require careful consideration and planning before implementation.

## Works Cited

"Background on Biometric Passports." *Privacy International*. 30 March 2004. 8 March 2009

<[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-61327](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61327)>.

Bain, Ben. "United States, Germany Will Share Biometric Data." *Federal Computer Week*. 11

March 2008. 8 March 2009 <<http://fcw.com/articles/2008/03/11/united-states-germany-will-share-biometric-data.aspx>>.

*Biometrics at the Frontiers: Assessing the Impact on Society*. Publication. 2005. Page 1. Institute for Prospective Technological Studies. 8 March 2009

<<http://66.102.1.104/scholar?hl=en&lr=&q=cache:9tTb3UCoGGcJ:www.informatica.pt/servicos/informacao-e-documentacao/biblioteca-digital/infraestrutura-do-software/seguranca-do-software/Biometrics%2520at%2520the%2520Frontiers.pdf+>>.

*Biometrics Portal*. 28 September 2005. 8 March 2009

<[http://www.europeanbiometrics.info/resources/details.php?Id\\_taxonomy=80](http://www.europeanbiometrics.info/resources/details.php?Id_taxonomy=80)>.

"Commission Proposes Inclusion of Biometric Identifiers in EU Citizens' Passports." *Rapid-*

*Press Release-Europa*. 18 April 2004. 8 March 2009

<<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/04/236&format=HTML&aged=0&language=en&guiLanguage=en>>.

Cross Match. "Biometric Identity Leader." 2009. *Cross Match*. 12 March 2009

<<http://www.crossmatch.com/>>.

European Biometrics. "European Biometrics Portal: Biometrics in Europe." 2005.

*European Biometrics*. 12 March 2009

[http://www.europeanbiometrics.info/news/newsdetail.php?Id\\_news=17](http://www.europeanbiometrics.info/news/newsdetail.php?Id_news=17)>.

"The Fingerprints." *The Federal Ministry of the Interior*. 1 December 2007. 8 March 2009

[http://www.en.bmi.bund.de/cln\\_012/nn\\_122730/sid\\_0B5C7BB989EE50E6B73E6D16965523BF/Internet/Content/Themen/Travel\\_\\_ID\\_\\_Documents/Electronic\\_\\_Passport/Fingerabdruecke\\_\\_en.html](http://www.en.bmi.bund.de/cln_012/nn_122730/sid_0B5C7BB989EE50E6B73E6D16965523BF/Internet/Content/Themen/Travel__ID__Documents/Electronic__Passport/Fingerabdruecke__en.html)>.

"Integration of Biometric Features in Passports and Travel Documents." *Activities of the EU*. 28

April 2008. 8 March 2009 <http://europa.eu/scadplus/leg/en/lvb/114154.htm>>.

Just 4 Business. *Biometrics Market Offers Huge Opportunities to Companies*. 2007.

*Just 4 Business*. 12 March 2009 <http://www.just4business.eu/2007/10/biometrics-market-offers-huge-opportunities-to-companies/>>.

"New, Secure Biometric Passports in the EU Strengthen Security and Data Protection and Facilitate Travelling." *Rapid-Press Releases-Europa*. 29 June 2006. 8 March 2009 <The European Union Requires Its Member States to Begin Issuing Biometric Passports by August 2006>.

Haubrich, Dirk. "September 11, Anti-Terror Laws and Civil Liberties: Britain, France and Germany Compared." *Government and Opposition*. 38.1 (2003). 3-28.

Ng-Kruelle, Grace, Paul A. Swatman, Douglas S. Rebne, and J. Felix Hampe. "The Price of Convenience: Developing a Framework for the Analysis of Privacy Sensitivity in the Adoption of Wireless Applications." *Proceedings of the 16<sup>th</sup> BLED International Conference on Electronic Commerce*. Ed. R.T Wigand, Y.-H Tan, J.E. Gricar, A. Pucihar, and T. Lunar. Bled, Slovenia, 9-11 June 2003. 480-500.

Oezcan, Veysel. "Germany Weighs Biometric Registration Options for Visa Applicants.

*Migration Information Source*. July 2003. 8 Mar 2009

<<http://www.migrationinformation.org/Feature/display.cfm?ID=141>>.

Revett, Kenneth. "Behavioral Biometrics." *Wiley Inter Science*. 24 Nov 2008. 12 Mar 2009

<<http://www3.interscience.wiley.com/cgi-bin/bookhome/121534398/>>.

Unisys. "Unisys Public Case Study: Malaysia Smart Card." 2002. 12 Mar 2009

<<http://www.uni->

[koblenz.de/~iwi/publications/aghampe/NgkSwaHamReb\\_2005\\_Biometrics\\_COLLECTeR-](http://www.uni-koblenz.de/~iwi/publications/aghampe/NgkSwaHamReb_2005_Biometrics_COLLECTeR-Europe.pdf)

[Europe.pdf](http://www.uni-koblenz.de/~iwi/publications/aghampe/NgkSwaHamReb_2005_Biometrics_COLLECTeR-Europe.pdf)>.