

---

## Foreword

It is the Spring of 2013, the insurgency in Ghazni Province, Afghanistan remains active, regularly targeting U.S., Coalition and Afghan National Forces with small-arms attacks and roadside bombs; attacks which often result in injury or death of soldiers. The insurgents in the area are local and blend in very well with the rest of the population. In fact, many of the insurgents work and associate with the U.S. and Coalition Forces on a friendly basis throughout the day, and execute their nefarious acts at night, in the absence of coalition presence. They do this effectively because they operate within the anonymity of the battlefield.

Over the last two months, we have seen an increase in improvised explosive devices in the vicinity of Ghazni City. One of my squads, while on joint patrol with the Afghan Uniformed Police, discovers an IED along their route. They investigate it with the assistance of the Explosive Ordinance Disposal team and continue their mission. The device is transferred to our forensic labs, where fingerprints are gathered and entered into our military biometrics database. While there is no identity associated with this file, we now have a fingerprint that we know is associated with an individual tied to the insurgency. Now the anonymity of the insurgent is at risk because we maintain a unique biological trait of his.

Approximately a month later, this squad is again working with the AUP, assisting them in recruitment of citizens into the police force. The soldiers are utilizing the Biometric Automated Toolset and Handheld Interagency Identity Detection Equipment to gather the biometrics of the recruits, capturing biographical data, photographs, fingerprints and an iris scan.

Biometric enrollment is common in the area and my soldiers consistently collect biometric data on the locals, villagers, policemen, etc. However, this day is a bit different. When one of the recruit's fingerprints is entered into the HIIDE a notice appears on the screen identifying the individual as a match against a fingerprint of a suspected insurgent and IED maker. The Biometrics Enabled Watch List quickly allows the soldiers to use this individual's biometrics (fingerprint) to remove his anonymity and identify him as a suspected insurgent. As a result of the biometric match, the individual is detained, his cache of weapons and several associates are captured and lives are saved.

While the story above may appear remote and far removed from the reader of this book, since the events took place in a province of Afghanistan, thousands of miles away, the reality could not be any further from the truth.

The world of the twenty-first century is filled with magnificent opportunities, technological advancements, life saving discoveries, and the ability to gain a global perspective in the blink of an eye via the Internet or fast global transit. However, with these incredible advancements and opportunities comes the uncertainty and complexity of a world that is more homogenous than ever and therefore also potentially more dangerous. The days of feeling sheltered and safe, based upon geographical separation, are no longer realistic as the threat can quickly and anonymously move from city to city, nation to nation, and even continent to continent.

The threat we face today is ever-evolving and highly mobile. Transnational crime, terrorism, fraud, weapons and narco-trafficking are here to stay. They are invading our societies putting our citizens at risk physically and financially. These threats keep militaries, law enforcement, and government agencies full of activity, seeking solutions, as they strive to counter this threat.

The most significant aspect of the threats discussed above is the anonymity of perpetrator. With over 7 billion people on the planet, the ability to counter the anonymity of the threat is essential to the protection of our societies. This is where biometric technologies and solutions can assist in eliminating the anonymity advantage as demonstrated in the vignette from Afghanistan.

While biometrics is generally misunderstood by the general population, outside of what they have seen from Hollywood films, the reality is that biometrics have been around for centuries. They are evident in the prehistoric hand prints in caves to the Old West's wanted posters with a picture of the culprit and the explicit notice "WANTED". These are a few examples of early forms of signature analytics and facial recognition. While Hollywood has done a good job bringing types of biometrics into the vernacular, it has done little to actually educate the general populace on the facts, myths, issues and benefits that surround their use, often resulting in either an irrational fear of the capability or an overly confident acceptance of the capability.

Even though fingerprints have been used in policing since the early twentieth century and simplified facial recognition for centuries before that, it has only been within the past two decades that the biometrics explosion has really started. One of the primary catalysts to this expansion in biometric capabilities, research and development was the wars in Iraq and Afghanistan. While fingerprints, iris scans, hand writing, facial recognition and DNA have been used prior to 2001, their use was mostly limited to use by law enforcement agencies.

Biometrics offers so many possibilities to assist and protect society, it is essential that they are understood and properly utilized. It is this basic principle that inspired Julian Ashbourn to develop his latest book, *Biometrics in the New World*. Through this work, Julian educates the audience about biometrics, makes certain the reader understands how and why biometrics should be used, and most importantly the necessity to do so in a systematic, ethical and collaborative manner.

Ashbourn expertly takes the reader through a comprehensive journey into biometrics to include the good, bad and the future of the capability. This is extremely important for the reader, whether a novice, technical expert, corporate executive or security official trying to determine how best to utilize this "new" capability to help safeguard and secure their investments or population. The bottom line is, biometrics

is here to stay and it is imperative that people learn now what its capabilities and limitations are.

The development, standardization and implementation of biometric capabilities, across the NATO Alliance, are a key priority. With the understanding that all of our operations are in some way human centric, it becomes important that we better understand the human dimension and characteristics in order to create the mechanisms required to use this information to counter anonymity and to safeguard our citizens and nations.

We are also very cognizant that any biometrics program must maintain security, privacy and account for the concerns and desires of the 28 member-nations as well as its partners. The Alliance's concerns with regards to Personally Identifiable Information, standardization, doctrine and Rules of Engagement are essential to the biometrics' Program of Work and framework for biometrics in support of operations. As the Biometrics Chief for SHAPE, I am working in concert with the goals and objectives addressed in *Biometrics in the New World*. Ashbourn is indeed an expert in biometrics, tremendous ally, contributor to the Biometrics program within NATO, and a mentor and guide to me as I continue to work with all our partners to further define, develop and expand Biometrics within NATO.

Ashbourn expertly addresses the current and future challenges that face society. Biometrics are here to stay and there is no going back. This is particularly evident in the communications industry, namely by Apple Inc. with its iPhone 5S, which has integrated a fingerprint scan to improve security, and by Samsung which is developing an Iris scanner for its new Galaxy 5S. Historically, once Apple and Samsung make something mainstream, it tends to be woven into the mesh of society. It is possible that these companies have ushered in the biometrics era to the general population because they bring acceptance through consumerism versus a government program or mandate.

However, moving too fast and without the right standards, protocols and privacy factors, biometrics programs throughout the world could become a nightmare. Rather than securing people, privacy, property and resources, biometrics will place all these things at risk unless systems and standards are put in place to ensure success. It is this aspect that the author so clearly expresses in these pages.

I strongly encourage our audience to carefully read the entire book to gain context on biometrics, its challenges and the benefits, while taking in every detail and internalizing the lessons and concepts that Ashbourn provides. By doing so, you will develop an understanding, which assist further development of safe and effective biometrics that are designed to secure society and not hinder it. Furthermore, upon reading *Biometrics in the New World*, you will become an informed consumer and contributor, far beyond your contemporaries, to one of the most significant technological programs of the twenty-first century.

Biometrics Chief, SHAPE HQs  
Lieutenant Colonel, USA

Stephen E. Gabavics

---

## Foreword

Today, we cannot live anymore without technology. Technology masters our entire lives. Completing simple tasks, such as defrosting food in the microwave, withdrawing money at an ATM, making a reservation for theatre tickets or applying for a new passport, all involve an important role for technology.

If technology stopped working, our whole society would come to a standstill and panic would ensue. In such a situation, would we have the common sense to find another way, a solution disconnected from technology? This brings me to the human factor. In too many situations technology is developed to work on its own and the user only has to follow the instructions and go step-by-step through the directions on a screen to receive a service. The key word in technology is standardization, and without standardization it is impossible to use technology in a proper way. This means that a system will remember, correct, verify, follow, decide, advise, and deny, and the user will simply follow and accept the outcome of the decision made by the system. This has an enormous impact on the brains of every individual from young to old. For example—how many people can remember more than 5 telephone numbers—while in the past every person had at least 20 different phone numbers stored in their brain? How many people are able to do a simple calculation off the top of their head without using the calculator on their smartphones? How many people can find their way to a certain address without using the GPS on their smartphone or in their car? Will the usage of all this technology have an influence on the citizens of tomorrow? Will citizens become standardized individuals with preprogrammed human software installed in our brains? Is this our future or is it time that we recognize this, change our course and start to develop more sophisticated tools to support our daily lives?

To achieve this we need someone who will wake us up, shake us and inform us of alternative human and societal solutions to cope with the current trend. Someone who has been trying to inform us for years about the risks and challenges of using technology without a proper pre-thinking process is Julian Ashbourn, the author of this book: *Biometrics in the New World*. Julian cares for people and nature, and really understands the impact of carelessly developed systems and software, that do not consider the human factor, on the independent individual. The success of a system is not related to its level of sophistication—but rather it depends on how the human factor is handled and integrated into the whole process. I am a strong supporter of using technology, but technology should support human beings and it

is the human being who should make the final decision. Not all dimensions of the lives of human beings can be integrated into a system, and so there will be always situations which it cannot be handle.

How best to integrate human and social factors into complicated systems such as biometrics, data collection systems, reservation systems and financial networks is explained in a clear and understandable manner for everyone in this book. I strongly encourage those who are involved in developing or maintaining such systems to put their I-Tablet aside, pick-up this book and spend a few hours learning more about how to develop and implement successful systems which will truly support us as human beings, stimulate our rational thinking and leave the final decision to us.

Senior Regional Officer for Border & Identity Solutions  
Head, Immigration and Border Management Unit  
IOM Regional Office for Asia and the Pacific  
Bangkok, Thailand

Sjef Broekhaar

Biometrics in the New World

The Cloud, Mobile Technology and Pervasive Identity

Ashbourn, J.

2014, XXI, 236 p. 12 illus., 11 illus. in color., Hardcover

ISBN: 978-3-319-04158-2