Biometrics and Consumer Electronics: A Brave New World or the Road to Dystopia?

By Peter M. Corcoran

Biometric systems confirm a person's identity by extracting and comparing patterns in their physical characteristics against computer records of those patterns. Examples include scans of the face, iris, or retina; measurements of hand geometry, palm or finger vein patterns; fingerprints, ear structure, voice patterns, or any other characteristic of the physical person that represents a unique attribute. The extracted patterns are matched against previously registered patterns, and, within certain tolerances, a confirmed match can be used to authenticate an individual's identity. In most practical systems, there is a need for a large, centralized data repository for storing the registered patterns, and substantial computing power is often required to process new patterns and compare these to the stored data set.

THE HISTORICAL ORIGINS OF BIOMETRICS

As with many of today's technologies, the history of biometrics stretches back further than we might think. One of the fathers of biometrics was a French police officer, Alphonse Bertillon, who developed an anthropometric identification system for suspects in the 1880s. His techniques were based on measurement of the characteristics of the head and body as well as individual marks such as scars and tattoos (Figures 1 and 2). These characteristics were processed to provide a unique identifying formula for each police offender.

First introduced into practical use in 1882, Bertillon's system was used in 1884 to confirm 241 repeat offenders in the Paris area. Its use was then widely adopted by the French police force. Although the system was later shown to be flawed because different police officers would implement measurements in slightly different ways, it was widely adopted in France and other European countries and later by U.S. and U.K. police. In France, it was popular enough that it was widely used even after the advent of fingerprinting. Bertillon was also responsible for the standardization of the police mug shot and did pioneering work on "metric photography," which he intended to use to reconstruct the dimensions of a particular space and the placement of objects in it.

> People are generally suspicious of biometrics and, if biometrics are not introduced carefully into a work environment or operational application, these suspicions can be sufficient to lead to failure. In practice, there are far more failures than successes.

Fingerprinting is one of the earliest biometric techniques. In fact, fingerprints were used as signatures in ancient Babylon. However, the first scientific research began in the 17th and 18th centuries. Nehemiah Grew (1641–1712) published the first scientific paper to describe the ridge structure of the skin covering the fingers and palms [16]. A century later, in 1788, the German anatomist Johann Mayer (1747–1801) recognized that fingerprints are unique to each individual.

In modern times, fingerprints were first used as a form of legal authentication in July 1858, when Sir William James Herschel, chief magistrate of the Hooghly district in Jungipoor, India, first used fingerprints on native contracts [17]. On a whim, without thought toward personal identification, Herschel had Rajyadhar Konai, a local businessman, impress his handprint on a contract. The idea was merely "to frighten [him] out of all thought of repudiating his signature." Herschel subsequently made a habit of requiring palm prints—and later, simply the prints of the right index and middle fingers—on every contract made within his district.

Juan Vucetich made the first criminal fingerprint identification in 1892 [17]. Vucetich, an Argentine chief police officer, created the first method of recording the fingerprints of individuals on file, associating these fingerprints to Bertillon's anthropometric

Digital Object Identifier 10.1109/MCE.2013.2239152
Date of publication: 28 March 2013

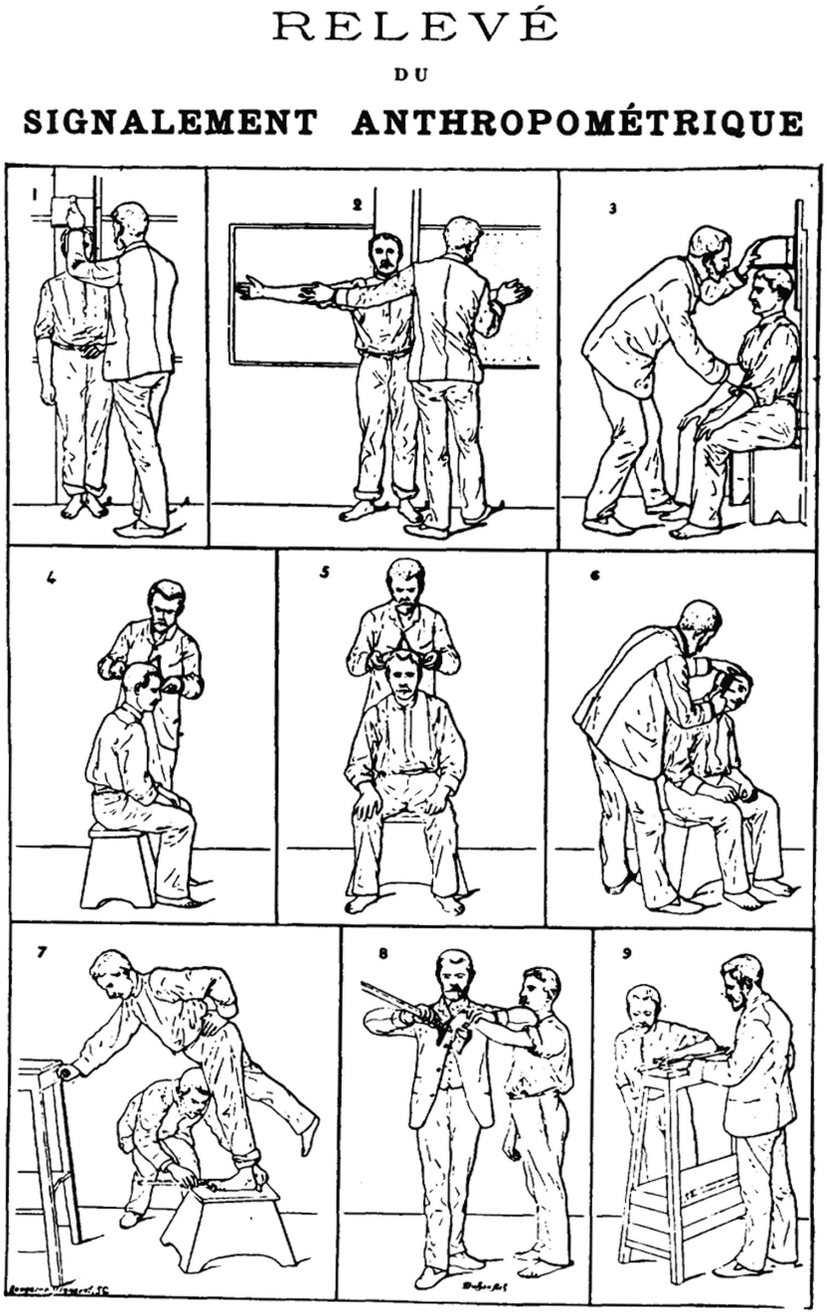


FIGURE 1. From Bertillon's *Identification Anthropométrique* (1893), demonstrating the measurements needed for his anthropometric identification system.

system. In 1892, after studying Galton's pattern types, Vucetich set up the world's first fingerprint bureau. In that same year, Francisca Rojas of Necochea was found in a house with neck injuries, while her two sons were found dead with their throats cut. Rojas accused a neighbor, but despite brutal interrogation, this neighbor would not confess to the crimes. Inspector Alvarez, a colleague of Vucetich, went to the scene and found a bloody thumb mark on a door. When it was compared with Rojas' prints, it was found to be identical with her right thumb. She then confessed to the murder of her sons [18]. The interested reader will find many additional details on the history of fingerprints in [17] and [18].

BIOMETRICS IN MOVIES AND POPULAR CULTURE

In 1882, Mark Twain (Figure 3) wrote, in *Life on the Mississippi*, about how a murderer was identified by his fingerprints. In one of his later books, *Pudd'n Head Wilson*, there was a dramatic court trial focused on fingerprint identification.

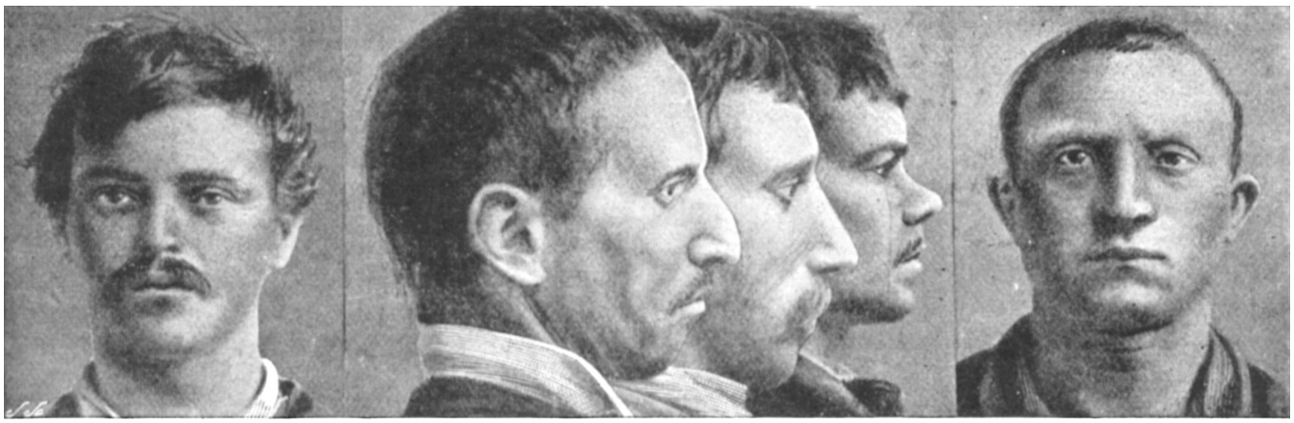
Biometrics in various forms has frequently been featured in science fiction literature and was also explored by mainstream authors, including George Orwell, Aldous Huxley, Philip K. Dick, Ray Bradbury, and William Gibson. In most of these works, biometrics was often employed as a method of restricting and controlling citizens, and the portrayals of a society that employs biometrics are invariably quite negative.

These trends have continued in recent movies. In *Minority Report*, a movie adaptation of a Philip K. Dick short story, the principal character is forced to have his eyes surgically replaced to prevent identification. In *Gattaca*, a 1997 movie directed by Andrew Niccol, the principal character must carry samples of another person's genetic material with him on a daily basis to pass a range of authentication protocols.

Strangely enough, these futuristic visions are not that far removed from today's technologies. We will discuss shortly how Sarnoff Corporation, Princeton, New Jersey, has adapted current technology using an array of cameras to enable iris recognition "on the move." This bears striking similarity to the scanning of a customer's iris patterns in the shopping mall scenes of *Minority Report*. The future is often closer than you might think!

PRACTICAL PROBLEMS IN THE DEPLOYMENT OF BIOMETRIC TECHNOLOGY

New deployments of biometric technology often turn out to be both complex and costly. Typically, the



The nose, as it cannot be disguised, is extremely important in identification. The types above, taking them from the left, show a low, narrow nose, a hooked nose, a straight nose, a snub nose, and a high, wide nose.

FIGURE 2. (a)–(c) Illustration from "The Speaking Portrait," an article in *Pearson's Magazine*, 1901, showing the principles of Bertillon's anthropometry.

technology suffers from acceptance and adoption issues. People are generally suspicious of biometrics, and, if biometrics are not introduced carefully into a work environment or operational application, these suspicions can be sufficient to lead to failure. In practice, there are far more failures than successes. For the interested reader, there are case studies and detailed discussions of the details of biometric deployments in [1].

A review of legacy deployments will quickly reveal that, while biometric technology appears attractive on first consideration, there are many real-world issues that both complicate and increase the costs of such deployments, not the least of which, issues of confidence and reliability in the underlying technologies can surface.

Complexities arise because not all biometrics are completely effective—there are people who cannot be fingerprinted due to injuries or scars and people who do not have a discernable iris pattern for genetic reasons; while these are outliers, they do preclude the use of biometric technologies for some individuals.

A further drawback of legacy technologies is that they lack convenience and comfort. People would have to comply with an acquisition process that required holding their face, eye, or hand in a certain position and often experiencing some physical or philosophical discomfort during this process. Nevertheless, there are successful examples of biometric deployment.

Another issue that arises with biometric data is that they cannot be revoked. The Electronic Freedom Foundation explains this very nicely [4]:

> In the near future, biometrics could stand in for your driver's license or social security number, and you could be asked for a thumbprint or an iris scan just to rent an apartment or see a doctor. This could lead to many vulnerable copies of that linked data that could wind up in the hands of identity thieves. And any data compromises would be catastrophic; unlike a credit card or even a social security number, your biometric data can't be revoked or reissued.

Nevertheless, in the last decade, biometrics has become increasingly practical as a means to identify and authenticate people across a range of applications and use cases.

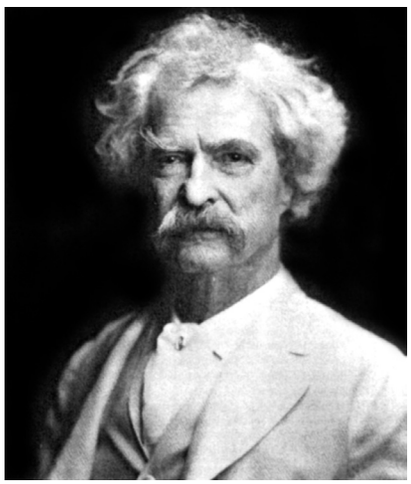


FIGURE 3. Mark Twain wrote about fingerprint identification in the 1880s.

In other words, if someone gains access to your fingerprint, or rather the digital pattern generated by it, he or she can obtain access to any services secured by that biometric data. And, unlike the PIN associated with your bank card, you cannot revoke and reissue biometric data—a very significant drawback in practical use. Thus, the widespread use of biometrics to control and manage authentication actually represents a significant risk and is likely to increase the incidence of identity theft and associated crimes.

EXAMPLE CASE STUDIES

Nevertheless, in the last decade, biometrics has become increasingly practical as a means to identify and authenticate people across a range of applications and use cases. Let us examine some well-known examples that will serve as a basis for later discussion.

Google uses iris recognition to control access to its data centers. Most currently available iris recognition systems impose substantial constraints on subject position and motion during the recognition process. The image-acquisition process largely drives these constraints, rather than the particular pattern-matching algorithm used for the recognition process.

While this is acceptable in a secured working environment, it would be less suitable in an open, semipublic environment such as an airport. Thus, Sarnoff Corporation has adapted current technology using an array of cameras to enable iris recognition on the move. As users walk through a short passage, their face region is captured by an array of multiple cameras under assistive lighting. An optimal iris image can be obtained by selection from these multiple images, requiring a single contactless walk-through by an individual (Figure 4). A YouTube video can be found at http://www.youtube.com/watch?v=b1uZonksCnI.

Another high-profile use of biometric technology is by Disney, who uses fingerprint recognition technology in its theme parks to combat the reselling of tickets. On entry, each ticket is associated with the ticket holder's biometric data so that it is not possible to resell the ticket after leaving the theme park. Fingerprint recognition is a well-known biometric and has been used for many years by police forces worldwide. As it requires a voluntary acquisition, it is less invasive of privacy than facial recognition. This is a good example where the barriers of acceptance and adoption have been overcome, allowing a successful deployment of the technology (Figure 5).

Naturally, there are other deployments, particularly by government and state agencies, where comfort, acceptance, and adoption are minor considerations. Thus, the U.S. Citizenship and Immigration Services make extensive use of biometric technologies—both fingerprint and facial images—to track people entering the country. People do not have a choice and must allow themselves to be scanned if they wish to enter the United States.

CONSUMER ELECTRONICS: A NEW ENABLER FOR BIOMETRICS

Consumer technology has progressed significantly in the last decade. New smartphone devices and tablet computers are disrupting traditional media and entertainment industries. Improvements in digital imaging and wireless networking technologies have turned these new mobile devices into powerful multimedia engines not only for viewing but also for generating content. Location services and social networking technologies enable these devices to link us geographically with our personal community of family and friends.

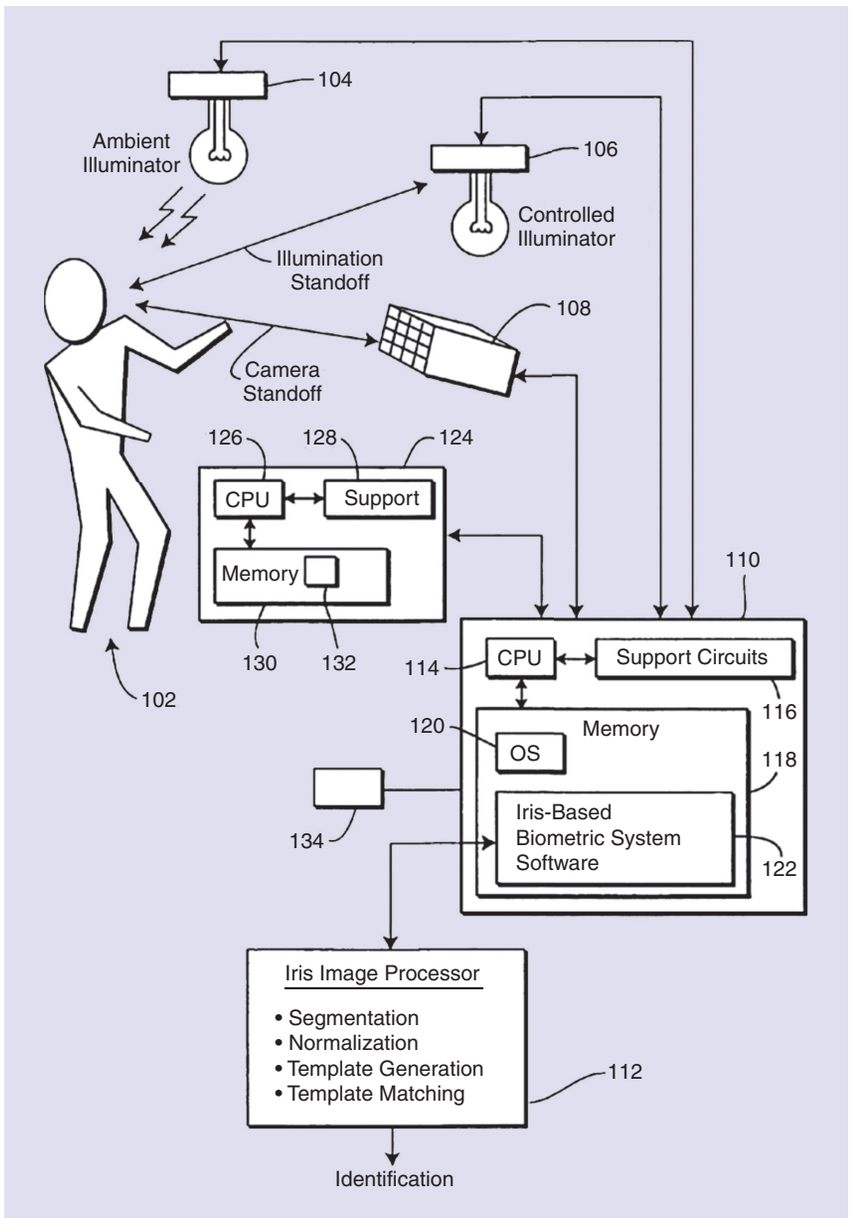


FIGURE 4. Iris recognition for a moving subject. Note the use of a parallel camera array (108) to capture multiple iris images simultaneously. (Image taken from U.S. patent 7,627,147, "Method and apparatus for obtaining iris biometric information from a moving subject.")

The growth rate for tablet devices exceeds that for the personal computer in the 1980s by an order of magnitude [2]; it is three times faster than the rate at which people have signed up for Facebook since it went public in 2007. That is a lot of tablets—640 million as of July 2012.

SMART IMAGING

We are on the cusp of a smart-imaging revolution. High-end digital cameras have leveraged the SLR architecture and larger sensor geometries to provide high-quality digital images. However, today's consumer cameras can deliver similar quality in a smaller footprint by combining multiple images to generate high dynamic range images. Real-time processing and analysis of the image stream is now commoditized with correction of flash-eye defects, face tracking, and beautification, smile, and blink detection being standard features in most consumer cameras and now appearing in smartphones as well.

The latest chip sets have dedicated hardware and even GPU subsystems embedded on chip with the main CPU. Data buses are optimized for full high-definition video at 60 frames/s; some can achieve even higher frame rates. In the near future, new optics technologies will overcome the limitations of the small lenses on these devices. The latest MEMS technology will provide a low-cost, miniature lens module with ultrafast focus and focus range from 10 cm to infinity.

SMARTPHONES

The sales of smartphones dwarf those of tablets. In 2012 alone, the sales of latter were around 200 million units per quarter, or 0.8 billion units annually.**<AU: Kindly check whether the edited sentence retains the intended meaning.>**

What is most interesting is the pace at which the underlying technology is evolving. The computing power of the latest chip sets has increased, but more interestingly, the multimedia capabilities have been given huge boosts through specialized hardware and the recent incorporation of GPU cores. These capabilities imply that smart imaging will become a commoditized feature of smartphone platforms in the next year or two.

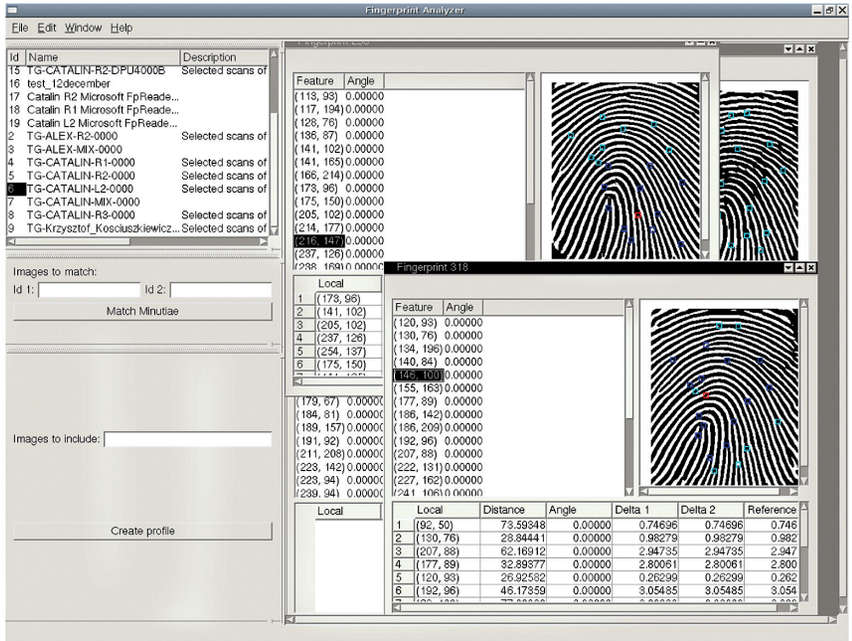


FIGURE 5. A fingerprint analysis toolkit. Note that the fingerprint images shown are preprocessed to enhance the ridge lines and determine the key points, or minutiae, in a robust and repeatable manner.

Also of interest is the transition from a desktop and keyboard culture to a touch- and thumb-based mobile lifestyle. Coupled with social networks and the powerful multimedia capabilities of today's hand-held devices, we are seeing significant disruptive social and economic effects arising from new usage patterns and user behaviors.

NEW SENSING TECHNOLOGIES

Location services have also become commoditized in our devices, thanks to advanced GPS chipsets and significant cost reductions as the technology entered mass-market electronic products. Today, your location is a key component of many services. Our devices also know and respond to their orientation, and it has become common to provide two video cameras to enable videoconferencing applications.

The touch-sensitive devices of today may soon be replaced by devices with three-dimensional (3-D) gesture-sensing capabilities. The Leap sensor (https://leapmotion.com/) can accurately follow detailed hand movements in a 3-D space above your desk. In case you doubt this evolution, a number of large corporations are already filing patents on 3-D user-interface concepts [3].

But what does any of this have to do with biometrics? Bear with me a little longer, we are getting there!

MAN OR DEVICE?

As I have already indicated, society is moving rapidly to the point where almost everyone will own a smartphone. In other words, perhaps more correctly, these smartphones will own us. They are compelling devices, combining the capability to act as a personal communications and messaging hub, a sophisticated personal entertainment device, and a life-log portal, should you require it.

The ability of a smartphone to augment our daily lives is already effecting substantial changes in social behavior. For many years, it was considered rude to leave your cell phone active in meetings; today, it is acceptable to tap away at this gadget in your hand. Indeed, it now seems to be considered impolite to interrupt someone while they are engaged in such, arguably antisocial, tapping.

And these behavioral adjustments are even more pronounced among the younger generation. For the youth of today, the smartphone is their principal social instrument. It is at the heart of their social lives and the center of their universe.

BIOMETRICS AND PRIVACY

This brings us to the interesting and key topic of biometrics and privacy. If we begin to use our personal biometric data as a means of authentication, it becomes very important to consider how these are used. The legacy approach, discussed above, typically gathers biometric data in centralized databases, and as we have also indicated, these biometric data cannot be changed. In effect, the owner of the data becomes the arbiter of your identity.

Clarke [13] has written in detail on this topic. He separates privacy into several subaspects and emphasizes the need for various safeguards, depending on the particular use of biometric data. These safeguards are essential if biometric technology is not to fall into ill repute even in relatively free societies. In more authoritarian societies, the worst fears expressed in popular culture may well become reality.

Jain and Nandakumar [14] focus more on the maturity of biometric technology but recognize the importance of considering privacy in any particular application of biometrics. More specifically, they raise several key concerns.

- Who owns the biometric data, the individual or the service providers?
- Will the use of biometrics be proportional to the need for security in a given application? For example, should a fingerprint be required to purchase a hamburger at a fast food restaurant or access a commercial Web site?
- What is the optimal tradeoff between application security and user privacy? For example, should governments, businesses, and other entities be able to use surveillance cameras in public spaces to covertly track benign activities of users?

There are many additional articles in the legal and philosophical literature that discuss various moral and ethical aspects of biometrics. But as the purpose of this article is not specifically directed to consider privacy issues, it is sufficient for the reader to be aware of these matters and the known concerns regarding the use of biometric technologies.

IDENTIFICATION VERSUS AUTHENTICATION

There are two major applications of any biometric recognition technology. Where a person claims a certain identity and his or her biometric data are used to verify this claim, this is known as verification or authentication.

If we can distinguish between the willing use of biometrics by individuals to prove their identity and the covert use of this technology without their knowledge, then many of the key privacy concerns are caused by inappropriate use rather than the technology itself.

It can be considered a user-driven technology, as the person will normally request access to a service or facility and agree cooperatively to provide the relevant biometric data. For example, presenting your passport at border control is an authentication process—the agent compares your face to the picture in the document.

Identification, on the contrary, is the task of determining an unknown person's identity. For example, a police officer comparing a sketch of an assailant against a database of previously documented criminals to find the closest match(es) is an identification process. Identification systems are often implemented covertly without the user's knowledge. Examples include determining the players at a gaming table in a casino, or checked-in passengers at an airport terminal, or people observed by street surveillance cameras.

The increasing use of public surveillance closed-circuit television systems in airports, train stations, and even on the high street has introduced significant potential for covert observation and tracking of individuals without their consent. While there are arguably benefits to law enforcement and immigration officials, it is the covert aspects of such systems that many members of the public find disturbing and that raise privacy concerns. If we can distinguish between the willing use of biometrics by individuals to prove their identity and the covert use of this technology without their knowledge, then many of the key privacy concerns are caused by inappropriate use rather than the technology itself.

RECOGNIZING PEOPLE

Most of us communicate on a daily basis using e-mail. While it is essentially an unsecured communication channel and can be easily intercepted and/or spoofed, this does not happen very often. The economic value of the vast majority of e-mails to a third party is negligible, and the nature of the social and business activities that most of us conduct does not make interception worthwhile. (There are significant exceptions, but we are mainly interested in the requirements of consumers rather than those of business or enterprise security.)

In the same vein, we do not require additional authentication for most of our e-mail correspondence or phone communications because we know the people with whom we are dealing, and they are identified by their e-mail address or phone number. In effect, we accept a machine identifier as sufficient for initial identification. It is true that we will subconsciously expect additional cues such as voice or writing style and will react to aberrations, but the initial authentication is based on the machine identifier.

Now consider the rapid adoption of smartphones and some of the likely consequences. With widespread adoption, we are already experiencing a rapid growth in new markets, applications, and services leveraging the technology, often in new ways. A significant proportion of these will lead to new market opportunities and a harnessing of the smartphone as an economic enabler. As new markets emerge and grow, some of these will become increasingly attractive to cyber criminals and, as technology continues to evolve, we should not expect that today's secure channels will remain secure. In the near future, you may no longer be able to trust simple machine identifiers as you do today.

COULD BIOMETRICS SOLVE THE RECOGNITION PROBLEM?

On first consideration, it would seem that adding a biometric to your e-mail address should offer a simple approach to authentication. If biometrics becomes commoditized in the near future, and this is certainly a key hypothesis of this article, then you would expect that incorporating your fingerprint or iris code into an e-mail would offer an elegant solution. Your laptop certainly has time to observe and scan your eye while you are composing that e-mail [15].

But we already mentioned that a key problem with biometric data is that they cannot be revoked. Thus, if every e-mail you send has your biometric data encoded into the mail signature, it would not take too much effort for a cyber criminal to access your biometric codes. And at that point, you are exposed to a risk of permanent identity theft. You cannot change your biometric data, so the thief has permanent access to your identity.

Once you understand this key point, you will realize why biometrics raises so many concerns and why there are so many issues related to its widespread daily use. There is a big Pandora's box here—if we get things right, then biometrics could address a wide range of new and emerging problems. But get it wrong, and we risk a major societal catastrophe.

AUTHENTICATION BY DEVICE

If biometrics is not a practical solution to tomorrow's authentication problems, what is the sense of this article?

In fact, while biometrics is not a solution on its own, it does form a key part of the solution. The problem of biometric data theft becomes significant when you store a biometric pattern in a central repository or database. If, however, the biometric data are used to generate an enrollment key and that is what is stored, rather than the biometric data itself, then this drawback is eliminated.

But you need something to generate this key, and this something must also be available later to decode the key and close the authentication loop. And as you would imagine, that something has to be quite generic and widely available.

In the near future, you may no longer be able to trust simple machine identifiers as you do today.

Remember all those smartphones we talked about? Yes, you guessed it—they provide the ideal middleman to close that authentication loop.

Yes, our smartphones are always with us. And we are talking on them and looking at them regularly every day. It is easy for them to hear us and see us. In our daily use of these devices, it is easy for them to acquire a range of our biometric data and build a detailed profile of the device user.

ADAPTIVE AND MULTIMODAL BIOMETRICS

Two synergetic approaches help to overcome many issues and drawbacks of legacy systems. Multimodal biometric systems use multiple sensors or biometrics. Unimodal biometric systems are limited by the integrity of a single identifier. It is unlikely that a multimodal system, employing several distinct biometric technologies (or a single biometric acquired with different sensors) will suffer from such limitations. The interested reader is pointed to Sahoo et al. [6] for detailed tradeoffs of response time, accuracy, and costs between integration modes.

Adaptive biometric systems aim to automatically update the templates or model to the intraclass variation of the operational data [5].

This research direction is expected to gain momentum because of some key advantages: 1) with an adaptive biometric system, one no longer needs to collect a large number of biometric samples during the enrollment process; and 2) it is no longer necessary to reenroll or retrain the system from scratch to cope with a changing environment. This convenience can significantly reduce the cost of maintaining a biometric system.

Now recall how the processing and acquisition abilities of smartphones have improved and continue to do so. These devices, suddenly endowed with multicore CPUs and dedicated GPUs have become capable of implementing complex algorithmic techniques that were once the privy of desktop engineering workstations or graphics-processing computer arrays.

The requirements for full high-definition video have endowed these devices with sophisticated video- and image-processing subsystems. In turn, these enable multiple biometric data to be extracted—face, iris, and hand shape—from video sequences. Additional sensory capabilities—motion sensing and location and voice recognition—provide auxiliary biometric data, enabling these devices to truly implement a multimodal approach to authentication. And smartphones are uniquely positioned to watch and listen to us on a daily basis, implementing an adaptive biometric approach to user authentication.

WHERE DOES SIRI FIT IN?

Perhaps the most interesting piece in this biometric puzzle is the Siri technology introduced recently by Apple.

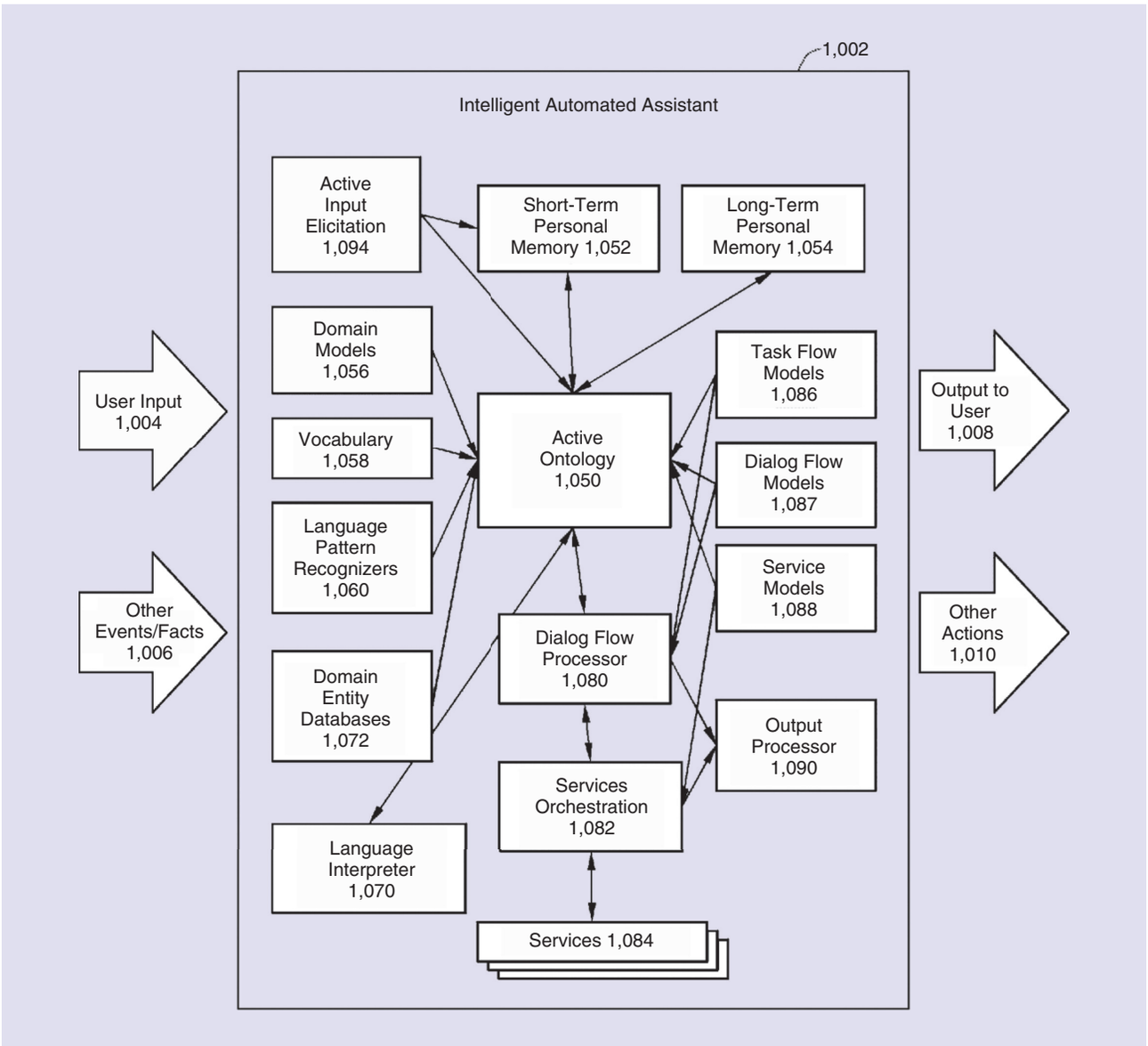


FIGURE 6. The core system components of Siri—an "intelligent automated assistant"; this includes learning capabilities to adapt to the individual user both in terms of services and how these are identified and actuated.

Many people regard Siri as another voice-recognition technology, but, in fact, a quick glance at the functional overview of Siri provided in U.S. patent application 2012-0016678 and shown in Figure 6 will reveal that there is a lot more to Siri.

Siri actually shifts a lot of data off the smartphone, which may seem counterintuitive given the processing capabilities of today's devices. But my guess is that Apple is using these data to determine broad patterns in the data of many hundreds of thousands of users. Note that key components in Siri are active; Siri will actively query the user when uncertain about input, and the core ontology is also in an active state of flux. A range of task, dialog, and service models will also, presumably, be in a constant state of change.

Siri appears to be a combination of learning and adaption "in the large," applied to customize and personalize the local device. The data from many users will improve the generic models and analysis engines built into Siri; at the same time, each user will have personalized customizations that are specific to his or her system.

Behind this, Siri should learn a great deal of person-specific behaviors, usage patterns, and task workflows. These would be more than sufficient to understand and track the normal device usage patterns for the primary user. And over time, these would allow building a capability to detect atypical use of the device.

THE "CLOUD" IS THE CATALYST

It is difficult to discuss consumer electronics devices these days without

mentioning cloud computing. Today, consumer devices are no longer an end in themselves. They can only succeed in today's marketplace by offering unique services, and these are invariably offered via a network connection. The huge success of the iPhone is matched by a step-function growth in network traffic. And today's devices are fast becoming inseparable from "the cloud."

But as we connect billions of devices to the Internet, new challenges appear. And new opportunities. Cloud computing offers some of the most significant examples. It enables the scaling of applications, services, and infrastructure, including storage. After all, our mobile devices are not going to be able to act on their own as stores for our growing digital assets.

Without a growing range of network services and applications, would these devices have become the compelling and pervasive instruments that now orchestrate our social lives and provide ever-present entertainment, communications, and digital recording facilities? Very soon, there will be more of these devices than there are people on the planet.

THE BLACK HOLE EFFECT

Music, movies, games, and now television are all finding new homes in the cloud. Many of us have already learned that it makes sense to have your personal image and video collections stored in a central location on the Internet, where they can be easily accessed from any device. This also makes sense when you consider the time and resources required to manage and store these digital assets at home.

The latest desktop applications have become increasingly integrated with the cloud. It only takes a touch of a button or ticking a checkbox to start the migration process for your pictures and home videos. Many of today's devices come with cloud connectivity built into the primary device workflows.

Not only does this overcome the limited storage capacity of today's devices, but it also facilitates the sharing and exchange of digital assets. Consumers no longer think about printing pictures when it is far easier to share them via the network or a Facebook page.

Slowly but surely, our data are being pulled online. Cloud services will continue to become smarter and more user friendly, and no one can deny the sheer convenience of having someone else worry about managing and storing your data. Resistance, as they say, is futile.

HOW SECURE IS THE CLOUD?

But as personal data migrate online, the focus must shift to the security and privacy of these data. It is clear that business data will require robust access protocols, and companies may even insist on encrypting sensitive data prior to uploading them. But companies are willing to pay for security and to train employees and enforce procedures in support of underlying security mechanisms.

Consumers are another matter. Although the general awareness of the public to security continues to grow, the sheer size and scale of basic phishing scams testifies to the gullibility of many consumers.

No matter how sophisticated the security mechanisms employed, the underlying vulnerability is the user. And no matter how broadly we seek to educate the public, it is clear that a significant proportion of device users will remain vulnerable.

Thus, while cloud security is an issue for commercial and professional users, it is practical to resolve security concerns for such users through conventional approaches. But for consumers and the general public who are about to become increasingly exposed to network-based applications and services, it is time to start thinking outside the box.

CONSUMER BIOMETRICS

And so, dear reader, we move to close the circle. As we can see, a new generation of connected consumer devices has arrived, riding on the back of an evolving global network infrastructure. These devices are so compelling and pervasive that they have become an instrument to gather and agglomerate all of our personal digital assets.

In turn, these are drawn, slowly but surely, to reside within a cloud-computing infrastructure that is also an early-stage disruptive technology. And it is a technology that was not designed to meet consumer needs or address the many issues of storing and sharing personal data and digital assets in a global networked environment.

In one sense, the security vulnerabilities and risks do not bear thinking (about). The sheer numbers of devices coming online and the size of the required support infrastructure alone are challenging. In addition, it is clear that conventional approaches are not likely to address adequately the many issues that will inevitably arise.

More specifically, consumers will choose convenience over compliance, so that applications and services that enforce awkward access protocols will not be successful in these markets, whereas those that put ease of use and simplicity first will succeed.

But at what cost? Will the security issues of connected devices and the cloud dwarf the problems we have today with desktop computer viruses, phishing scams, and online credit card theft? Or is there another way?

GADGETS TO THE RESCUE

Well, fortunately, as was indicated at the beginning of this article, these new devices are also equipped with very sophisticated sensing subsystems. And with increasing computational power, they have started to incorporate advanced image analysis, feature extraction, pattern recognition, and adaptive intelligence engines such as that employed by Siri.

Now coupled with the fact that we engage with our devices on a daily basis in different ways, employing multiple workflows, it becomes quite straightforward for a device to begin to "learn its user." Unlike desktop devices, we do not share mobile devices with other users, so there is a low probability of confounding factors for this learning process.

Yes, very soon your smartphone will be watching and listening to you. It will sense how you hold it and determine

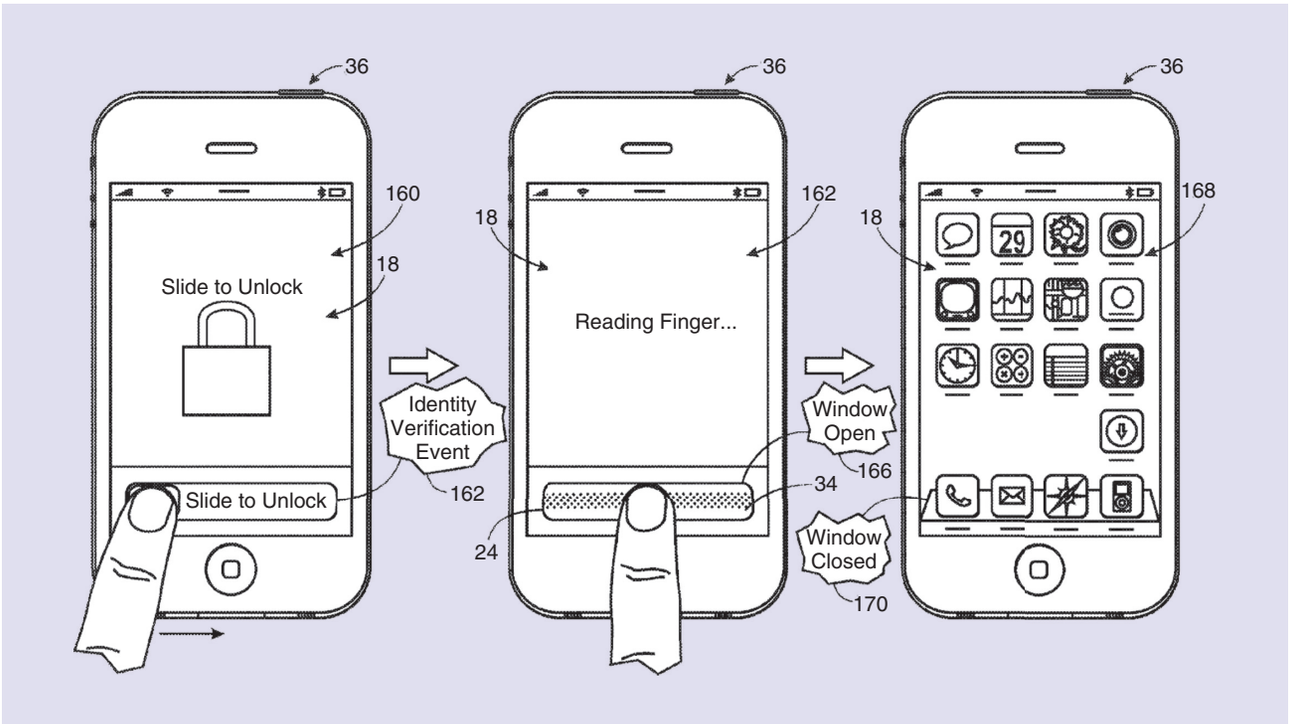


FIGURE 7. Repurposing of the finger swipe operation that is used to unlock some devices. Here, the bottom region of the display is modified to sense latent fingerprints so that the swiping operation captures the finger biometric data that are used to validate the user.

when and for how long you walk. It will be able to observe and analyze how you respond to texts and e-mails and recognize how you commence and terminate phone calls.

As you work with its touch-screen interface, the user-facing camera will capture and analyze your face and iris data over multiple image frames, enabling high-quality images to be constructed. Some touch interfaces could even capture your fingerprint patterns as you poke and thumb at them.

PRACTICALITIES: CAN IT WORK?

Of course, most of these capabilities are not yet realized as practical products or services. But they have all been shown or demonstrated at the proof-of-concept stage.

In fact, the latest smartphones already implement facial recognition and voice authentication [7]. More esoteric techniques such as gait analysis [8] and touch analysis [9] have been demonstrated as proof-of-concept. So the question is not if it can work but rather how soon?

If you doubt this, then consider Figure 7, which is taken from a very recently published patent application [10]. I am sure that you will recognize the device, but what is most interesting is that one key embodiment described in this document considers repurposing the use of the standard finger swipe action that unlocks the device. This is illustrated in Figure 7, which shows that this unlocking action is employed as a convenient means to acquire biometric data to confirm the user identity.

This is a standard workflow that is already familiar to the users of this device. By retaining such familiar aspects of the user interface, it is possible to introduce biometric validations as part of the normal device usage.

As long as the device continues to receive such validations—voice, face video, gait patterns, and text-based messaging are typically available several times daily—the device itself can provide authentication for a wide range of interactions with the cloud infrastructure.

REAL-MONEY TRANSACTIONS

Naturally, there will be certain operations, in particular what are known as "real-money transactions" (RMTs), that require an additional layer of user authentication. These are the equivalent of today's online banking, credit card, or PayPal transactions over the Internet (Figure 8).

Today, we type in a username, a password, and some additional alphanumeric code that may be fixed, but it is often generated using a third-party electronic key generator or a chip card. The use of a key generator removes the dependency of part of the authentication process on the desktop computer used to execute the transaction. Thus, even if the local computer is compromised, it is not possible for an attacker to generate his or her own keys, as he or she has no knowledge of the key generator.

For our mobile devices, there is no need for a key generator. Instead, we can simply use biometric data. As long as the biometric data are used to create a unique key [11] and the method of key generation is not disclosed,

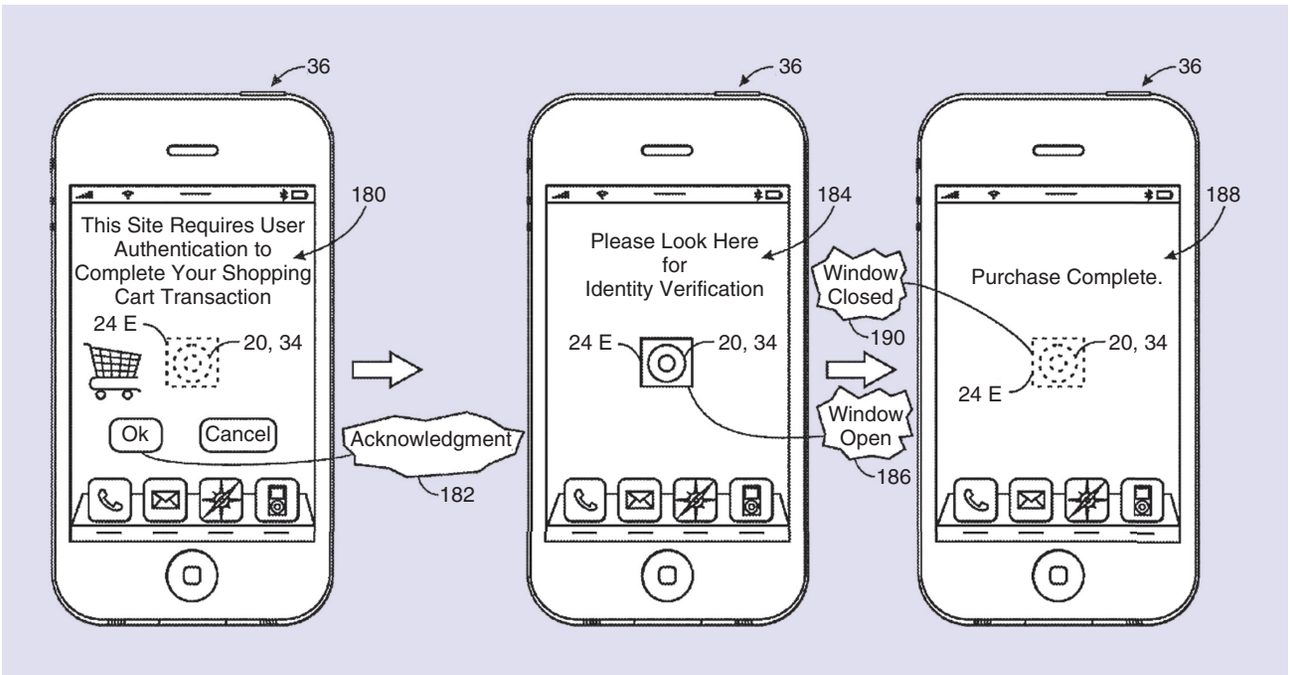


FIGURE 8. It is only a short additional step to use advanced biometrics such as an iris for authentication. Today's devices are capable of processing 60 frames/s and incorporate GPU units; thus, they can acquire and fuse multiple images to ensure high-quality biometric data.

a simple, yet secure and robust, authentication can be achieved using a trusted third party (TTP) architecture combined with zero knowledge proof (ZKP) techniques [12]. Thus, the extracted biometric feature(s) are protected by ZKP, and the transactions are verified via well-known TTP techniques.

WHO NEEDS THIS AND WHY?

The short answer is everyone. Businesses, retailers, and financial institutions need reliable means to establish authenticated connections with customers, both to protect their privacy and to validate transactions. Today's model of credit card numbers, PIN codes, and electronic key generators works, but it is awkward and lacks convenience for the consumer. If personal devices can provide improved convenience and biometrics can provide an improved user experience, then adoption will snowball. We are not there yet, but there is definitely something in the air.

As individuals, our lives have become increasingly entangled with the Web, socially, professionally, and economically. As this entanglement grows, we need new degrees of authentication. Today, an e-mail address is generally sufficient to provide authentication for most low-level interactions, but that is because the relative rewards for gaining access to a person's e-mail do not normally justify the risks and possible consequences. However, as more sophisticated tools and methods become available to cybercriminals to exploit emerging social infrastructures and communities on the Web, the consequences and incidents of low-level identity thefts are likely to grow. Eventually, they will reach a point where we need more than basic username/password authentication for day-to-day digital activities on the network.

As individuals, our lives have become increasingly entangled with the Web, socially, professionally, and economically. As this entanglement grows, we need new degrees of authentication.

Biometric back channels can provide continual verification that you are who you claim to be, even when simply chatting online, or participating in a teleconference. Social networks will need such tools as their membership grows and cybercriminals become more sophisticated. Indeed, many such businesses, including Facebook, see mobile devices as their future. Authentication via the device is icing on the cake!

At a slightly higher level of security, many of us will operate our business or provide professional services over the Internet. Again, where reputation is vital, professionals, small businesses, and service providers need to protect their identity and have reliable and practical means to authenticate themselves in multiple online environments and workflows.

Finally, we need authentication for RMTs. As our economy evolves further in the digital age, more earning and spending activities will occur online. Already, the bulk of banking transactions are initiated outside the control of internal banking networks.

We are in the age of Internet banking, but it is only a matter of time before conventional security is challenged. Biometrics, accessed via our mobile devices, provides a new approach to secure key generation and personal authentication.

BRAVE NEW WORLD OR DYSTOPIA?

The day of continual authentication by device is still ahead of us. There are many challenges and speed bumps on the road ahead. Nevertheless, with the right standards and some improvements and field testing of existing technologies, it is a realizable vision—and a desirable one for many.

It is clear then that the day when our devices will "know" us is not too far away. And when they know us, that capability will enable a wide range of improved services and businesses based on this new, robust authentication by device.

To achieve this, we are handing a lot of power and responsibility over to those devices. Once this process reaches a critical mass in terms of social and economic impact, that capability will only grow in its importance, embedding itself into the norms of our society.

But is this ultimately a good thing? Is it a good thing for us as individuals? What are we trading in terms of personal privacy and freedom for some extra convenience in our daily lives?

And as a society? Can it be a good thing to concentrate such power in our devices? Are we opening the door to a mass surrendering of personal privacy on a scale that was simply not possible before? There are many frightening visions of future societies that incorporate biometric technology that have been painted by classic science fiction authors; George Orwell, Aldous Huxley, Philip K. Dick, Ray Bradbury, and William Gibson have all dabbled here.

What is also interesting is that the control over consumer biometric technology does not rest with the government but with the device manufacturers. Ultimately, they will control how biometric technology is implemented and integrated into their devices or the underlying operating system that controls those devices.

It is already clear that different corporations have adopted very distinctive policies relating to their devices and device technologies. How will these evolve in the context of biometrics as an enabling technology? Will the government step in at some point to regulate such technologies? What access will government agencies have to the data itself and the encryption mechanisms?

What of those who choose not to engage with this brave new world? Could we someday find that it is illegal not to have a personal smart device? Could these devices become a requirement for day-to-day living, rather than an option? How would society handle biometrically challenged individuals?

There are many unanswered questions here. Let us see how the story of consumer biometrics unfolds during 2013. And if you have any thoughts on the matter raised in this "Soapbox," please consider writing an article for *IEEE Consumer Electronics Magazine*. Articles should be submitted to http://mc.manuscriptcentral.com/cemag by mid-May for the Fall 2013 issue, mid-August for the Winter 2013 issue, or mid-November for the Spring 2014 issue, to allow time for peer review. The editor may be contacted at cesmagazine@gmail.com (or cesmagazine@ieee.org if you prefer).

ABOUT THE AUTHOR

Peter M. Corcoran is the editor-in-chief of *IEEE Consumer Electronics Magazine*.

REFERENCES

[1] B. Rothke and B. Tomhave. (2012). The biometric devil's in the details. *Secur. Manage.* [Online]. Available: http://www.securitymanagement.com/article/biometric-devils-details-004961

[2] L. Meredith. (2012, Aug. 27). TechNewsDaily [Online]. Available: http://www.technewsdaily.com/4762-smartphones-and-tablets-poised-to-take-over-the-world.html

[3] P. M. Corcoran. (2012, Apr.). Understanding patent applications (IP corner). *IEEE Consum. Electron. Mag. 1(2)*. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6172457&isnumber=6172456

[4] [Online]. Available: https://www.eff.org/issues/biometrics

[5] A. Rattani, "Adaptive biometric system based on template update procedures," Ph.D. thesis, Univ. Cagliari, Italy, 2010.

[6] S. K. Sahoo, T. Choubisa, and S. R. Mahadeva Prasanna. (2012, Jan.). Multimodal biometric person authentication: A review. *IETE Tech. Rev. 29(1)*. Available: http://tr.ietejournals.org/text.asp?2012/29/1/54/93139

[7] D. Reynolds. (2012, May 3). Samsung unveils Galaxy S III smartphone with face, voice recognition. *CNN Tech* [Online]. Available: URL: http://articles.cnn.com/2012-05-03/tech/tech_mobile_ samsung-galaxy-s-iii-smartphone_1_samsung-smartphone-face-recognition-software?_s=PM:TECH

[8] M. Tamviruzzaman, S. I. Ahamed, C. S. Hasan, and C. O'Brien. (2009). ePet: When cellular phone learns to recognize its owner. presented at 2nd ACM Workshop Assurable and Usable Security Configuration (SafeConfig '09) [Online]. Available: http://doi.acm.org/10.1145/1655062.1655066

[9] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. (2012). Touch me once and I know it's you!: Implicit authentication based on touch screen patterns. presented at SIGCHI Conf. Human Factors in Computing Systems (CHI '12) [Online]. Available: http://doi.acm.org/10.1145/2207676.2208544

[10] F. J. A. Riviera, R. Hung, M. Dinh, and S. A. Myers, "Devices and methods for providing access to internal component," U.S. Patent 2012-0258773, 2012.

[11] C. Cucu, A. Cucos, and P. M. Corcoran. (2008, Jan.). Determining unique fingerprint features for biometric encoding of data. presented at Int. Conf. Consumer Electronics, 2008 (ICCE 2008) [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4588002&isnumber=4587847

[12] S. Grzonkowski, P. M. Corcoran, and T. Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services," in *Proc. Int. Conf. Consumer Electronics–Berlin (ICCE–Berlin)*, 2011, pp. 83–87. doi: 10.1109/ICCE-Berlin.2011.6031855

[13] R. Clarke. (2001). Biometrics and privacy [Online]. Available: http://www.rogerclarke.com/DV/Biometrics.html

[14] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy," *Computer*, vol. 45, no. 11, pp. 87–92.

[15] P. M. Corcoran, F. Nanu, S. Petrescu, and P. Bigioi, "Real-time eye gaze tracking for gaming design and consumer electronics systems," *IEEE Trans. Consum. Electron.*, vol. 58, no. 2, pp. 347–355, 2012.