EDITOR'S NOTE: BIOMETRICS, AND MORE!
Victoria Prusen Spears

BIOMETRICS IN THE WORKPLACE: KEY LESSONS FROM EMERGING CASE LAW UNDER THE ILLINOIS BIPA
David R. Singh, John Stratford, and Neeckaun Irani

YOU CAN'T CHANGE YOUR FINGERPRINTS, BUT DO YOU NEED TO? THE EVOLUTION OF BIOMETRIC- AND PASSWORD-BASED AUTHENTICATION SECURITY—PART II
David Kalat

SEC WARNS REGISTERED FIRMS ABOUT CLIENT PRIVACY AND DATA SECURITY
Natasha G. Kohne, Michelle A. Reed, Peter I. Altman, Diana E. Schaffner, and Nicole Ashley Greenstein

MASSIVE DATA BREACH UNDERSCORES IMPORTANCE OF BUSINESS ASSOCIATE SECURITY
Helen R. Pfister and Randi Seigel

PROPOSED CCPA AMENDMENTS SIGNAL CALIFORNIA LAWMAKERS' WILLINGNESS TO NARROW SWEEPING PRIVACY LAW
Xiaoyan Zhang, Gerard M. Stegmaier, and Kimberly J. Gold
Pratt’s Privacy & Cybersecurity Law Report

VOLUME 5  NUMBER 7  SEPTEMBER 2019

Editor’s Note: Biometrics, and More!
Victoria Prussen Spears 209

Biometrics in the Workplace: Key Lessons from Emerging Case Law Under the Illinois BIPA
David R. Singh, John Stratford, and Neeckaun Irani 211

You Can’t Change Your Fingerprints, But Do You Need To? The Evolution of Biometric- and Password-Based Authentication Security—Part II
David Kalat 217

SEC Warns Registered Firms about Client Privacy and Data Security
Natasha G. Kohne, Michelle A. Reed, Peter I. Altman, Diana E. Schaffner, and Nicole Ashley Greenstein 231

Massive Data Breach Underscores Importance of Business Associate Security
Helen R. Pfister and Randi Seigel 235

Proposed CCPA Amendments Signal California Lawmakers’ Willingness to Narrow Sweeping Privacy Law
Xiaoyan Zhang, Gerard M. Stegmaier, and Kimberly J. Gold 238
Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR
Victoria Prusse Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenigsberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Baker & McKenzie LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine
You Can’t Change Your Fingerprints, But Do You Need To? The Evolution of Biometric- and Password-Based Authentication Security—Part II

By David Kalat*

This two-part article seeks to synthesize key ideas in password- and biometric-based information security to help guide decision makers and stakeholders responsible for evaluating the risks and benefits of each. The discussion focuses on fingerprint-based biometric identification systems due to their ubiquity, but the principles illustrated by fingerprint-based examples are applicable to other biometric systems as well. The first part of the article, which appeared in the June 2019 issue of Pratt’s Privacy & Cybersecurity Law Report, discussed the five components of AAA security, the origin of password insecurity, the history of encryption, bitwise operations, the UNIX password protection scheme, hash collisions and salts, and brute-force attacks. This second part of the article covers biometric identification, the Bertillon System, fingerprints, biometric security, feature transformations, biometric cryptography, and hill-climbing and spoofing.

BIOMETRIC IDENTIFICATION

The term “biometrics” refers to measurements of human biological characteristics. Examples of biometric characteristics include fingerprints, face, iris, retina, skin spectroscopy, and DNA, as well as behavioral aspects such as gait analysis. One significant advantage of biometric-based authentication methods is that it directly ties the identification process to the subject’s actual identity, as opposed to a secondary attribute like a password. In order to pass a biometric authentication, the subject must be physically present. Biometric data cannot be forgotten, misremembered, or shared with a friend. It cannot be guessed or borrowed, and there is no risk of multiple users choosing the same fingerprint. However, the intimacy of the biometric data also heightens privacy and security concerns.

Structurally, a biometric-based authentication mechanism entails two critical phases. The first phase is “enrollment,” when a subject’s biometric data is first accessed to

---

*David Kalat is a testifying expert in electronic evidence and digital forensic investigations. He leads the Chicago digital forensics lab for BRG’s Global Investigations and Strategic Intelligence practice group. Mr. Kalat is a Certified Fraud Examiner, a Certified Computer Examiner, a Certified Information Systems Security Professional, a Certified Telecommunications Analyst, and a licensed private detective. (Footnotes continued from Part I of this article.)
derive statistical values that will be represented in a stored output called a “template.”

The second “authentication” phase follows the same process of accessing the subject’s biometric data to derive a second template, which is then compared to the stored template in a matcher module.  

Unlike a password-based system where the user can input the alphanumeric password identically every time, with perfect correspondence between the input value and the stored value, capturing biometric data is subject to numerous variables. For example, in the context of fingerprint scanning, a wide array of factors will influence the quality and condition of the fingerprint, including the cleanliness and dryness of the finger, is the skin cut or scraped, how hard the subject presses the finger onto the sensor, and environmental issues such as temperature and humidity. Given this inherently imprecise input, the matcher evaluates the similarity between the two templates and outputs a numerical value. If the similarity is above a certain predetermined threshold, the templates are considered to match and the subject is authenticated into the system.

Possible failures of biometric identification systems can be categorized into intrinsic versus external failures. Intrinsic failures occur when the system itself falls short of its intended application, and either fails to recognize a valid biometric input (false rejection) or authorizes an invalid biometric input (false acceptance). The relative false rejection and false acceptance rates is an overall measure of the accuracy and reliability of the system. The acceptable threshold for this balance will depend on the use case for the system—the standard for ensuring accurate identification of a subject for a financial transaction is different from a system that uses biometrics to configure preset radio stations in an entertainment center. External failures occur when the system is compromised by a malicious attacker. This can either result in the attacker gaining unauthorized access, or causing the system to deny access to its authorized users.

Research on biometric security tends to categorize different types of risks based on the aspect of the system that could be attacked, including:

1) Attacks on the input system involve the use of fraudulent or “spoofed” biometric credentials to gain access.

2) Attacks on the interface between the modules can jam, intercept, modify, or replay data as it is transmitted between system components.

---

3) “Trojan Horse” attacks on software modules can cause them to misbehave in ways beneficial to the attacker, such as rejecting all templates to deny access to all authorized users, or to cause the matcher module to output a valid matching score for a foreign template.22

4) Attacks on the template database can replace valid templates with modified ones, can steal templates with the intention of reversing them to spoof credentials for a subsequent attack on the input sensor, or steal credentials to be replayed into the system.

THE BERTILLON SYSTEM

The practical use of biometrics for identification began in the late 1800s in the field of law enforcement. French policeman Alphonse Bertillon described the idea in his landmark book of 1885, *Signaletic Instructions Including the Theory and Practice of Anthropometrical Identification*. Bertillon aspired to apply a rigorous scientific framework to the then-haphazard practice of tracking and cataloging criminals. Bertillon proposed to catalog individuals by specific measurements he presumed to be immutable attributes of the person: head length, head breadth, length of the middle finger, length of the left foot, and length of the cubit (the forearm from the wrist to the elbow). Bertillon posited that the combination of these measurements together with photographic face-on and sideways “mugshots” of the subject would provide a definitive identification of a unique individual. The photos and biometric measurements would then be printed onto a “Bertillon Card” to be stored in a library of criminals. This manually searchable database was an enormous boon to the field of criminology, and the “Bertillon System” quickly took hold across Europe and the United States.

It had a couple of notable drawbacks, however. For one, even Bertillon himself agreed that it was a grueling and time-consuming task to find a single face “if you have no other means but your eyes to search for the photograph among the thousands in an ordinary collection.”23 Second, the system was designed to be reactive, to help identify suspects and monitor repeat offenders, but did little to proactively prevent crime. The biggest problem, however, was the one that brought the Bertillon System to an end in 1903.

Officials at Leavenworth Penitentiary in Kansas were processing a new inmate, named Will West, and performed the usual Bertillon procedure of capturing mugshots and biometric measurements. Vexingly, his measurements matched exactly an existing Bertillon Card for someone named “William West.” This was especially puzzling

22 The term “Trojan Horse” has a slightly different inflection when used in biometric security contexts than it does in more general cybersecurity contexts.

because William West was already incarcerated at Leavenworth and had been for two years serving a conviction for murder. Here were two men, with basically the same name, strikingly similar appearances, and identical Bertillon measurements—yet they were indeed two different people, unrelated and unknown to one another. The prison officers fingerprinted both men to show their fingerprints differed, demonstrating the superiority of fingerprint identification.  

**FINGERPRINTS**

Humans leave latent copies of their fingerprints behind on almost any solid surface they touch, and generations of forensic examiners have learned how to recover and analyze them to identify the person to whom they belong.

The science of fingerprint analysis was codified by Sir Francis Galton in the late 19th century, culminating in the 1892 publication of his landmark treatise *Finger Prints*. Galton cataloged the unique characteristics, collectively called “minutia.” Fingerprints are composed of ridges and valleys of skin, and the organization and pattern of those ridges and valleys are biologically unique between individuals, even identical twins. The ridges and valleys form a variety of distinctive features, including arches, loops, whorls, islands, lakes, and other colorfully-named structures. The most important of these so-called “Galton Details” are cores (areas found near the center of loops and whorls) and deltas (triangular areas found in loops and whorls), collectively referred to as “singularities.” The relative position and orientation of these singularities is used to classify any given fingerprint into one of five distinct, non-overlapping classes, from which more refined analysis begins. If a comparison between any two fingerprints yields a high enough number of matching characteristics, the prints are considered to come from the same individual.

In order to systematize this process of fingerprint analysis into something that can be performed efficiently by computers, modern biometric systems eschew the identification of singularities altogether, and do not attempt to perform pattern matching on images. Instead, most commercial fingerprint-based biometric systems rely on mapping “minutia,” which are a particular subset of the Galton Points. Although fingerprint analysts have identified as many as 150 different types of minutia, only the points where ridges either terminate, or bifurcate are considered salient for the purposes of automated identification systems.

---

The FBI first began researching how to implement minutia-based fingerprint identification in 1969, collaborating with the National Bureau of Standards (now the National Institute of Standards and Technology) to develop effective technology. In 1975, the FBI deployed the first fingerprint scanners capable of extracting minutia. At that time, the high cost of digital storage necessitated storing templates with only the most essential information.\(^2\)

During the enrollment phase, a subject places her finger onto a device designed to read the ridges. Different manufacturers use a variety of competing sensor technologies including optical, capacitance, pressure, thermal, or ultrasound. Whatever sensor technology is used generates an image of the fingerprint, but this needs to be processed before it can be used to identify minutia points. First, the grayscale image is converted to a pure black-and-white image with no intermediate grays, and is “thinned” to reduce each ridge down to the width of a single pixel. The system then identifies minutia points by their orientation and coordinates on an x/y plane.\(^2\) The process of thinning and then extracting minutia points has a tendency to introduce false minutia into the template. Additional algorithmic processing is applied to filter false minutia from the template.\(^3\)

The template is saved to a database and is assigned to a particular user identity or account in the system in question. During the authentication phase, a subject presents her finger to be read and processed in the same way, and the resulting template is compared to a stored template by a matching module.\(^4\)

Research has shown that it is unlikely, if not impossible, to achieve a perfect match. The same finger placed on a sensor a hundred times in succession can produce a hundred distinct templates. Consequently, matching algorithms are designed to compare the similarities between the enrolled template and the one presented for authentication. The threshold of similarity can be calibrated by the system designer to balance the risks of false rejection and false acceptance to find the optimum balance of accuracy.\(^5\)

---


An attack on the sensor using fraudulent or fake credentials is called “spoofing.” In such a scenario, an unauthorized person presents a fake fingerprint of some kind to trick the system into granting them access.\(^{33}\)

**BIOMETRIC SECURITY**

Anil K. Jain, a University Distinguished Professor at Michigan State University and a leading researcher in the field of biometric security, proposes that the protection of a biometric template should address the following four principles\(^ {34}\):

1. **Security:** It should be computationally infeasible to reverse a protected template back to the original biometric data;
2. **Diversity:** If the protected template is obtained by an attacker, it should be impossible to use it in a different database or system;
3. **Revocability:** If a protected template is compromised, it should be straightforward to revoke it and replace it with a new protected template based on the same biometric data; and
4. **Performance:** The protection scheme used to achieve the previous three principles should not materially degrade the system’s false acceptance or false rejection rates.

For privacy and security reasons, the amount of information contained in a template should be limited to the minimum necessary to identify matches, without revealing data that would allow an attacker to replicate the original biometric trait.\(^ {35}\) Due to the limited amount of information captured in a template, the extent to which that information has been processed into a reduced set of coordinates, and the degree to which false minutia coordinates are introduced as a type of noise, it has historically been presumed that an attacker would be unable to reverse-engineer an original fingerprint from a template alone.\(^ {36}\)

In 2001, a student at the Australian National University examined this assumption and agreed that “due to the loss of information that occurs when a template is created, it is impossible to recreate the original fingerprint that was used to create

---


that template.” However, he found that a residual security risk persisted from the possibility of creating a synthetic fingerprint based on the template that could be used to spoof the sensor into granting access. His research demonstrated a technique for synthesizing a spoofed fingerprint capable of fooling the matching algorithm if the stored template contained both minutia and singularity information.37 In 2007, Anil Jain and fellow researchers Arun Ross, and Jidnya Shah showed that a fingerprint template containing only minutia coordinates (but no singularities) could also be used to generate a synthetic spoofed fingerprint. Although Ross et al. confirmed that a complete replica of the original fingerprint was not possible, the synthetic replica was potentially capable of being used to fool a sensor into authenticating the fake fingerprint.38

The concept of Revocability mentioned above refers to the principle that, in the event that one or more stored templates are breached or compromised, a secure system should allow the template to be canceled and replaced with a new enrollment. Different methods of creating and protecting cancelable templates have been proposed by various researchers, and different systems implement various combinations and variations on these ideas. In general, the techniques used to protect biometric templates can be classified under two principal categories. “Feature transformations” are methods of altering the template data before it is stored so that the stored template cannot be reversed back to the original biometric data. “Biometric cryptosystems” are methods of integrating biometrics into cryptography so that the template data is stored in an encrypted format. The two categories are not mutually exclusive, and systems may use a combination of these methods in a hybrid approach.39 These ideas are discussed in more detail below.

FEATURE TRANSFORMATIONS

There are two types of feature transformations (although there are numerous individual applications of these types). A “salted” transformation uses a technique similar to salting a hash, in that a separate piece of binary data is added to the template during the transformation. Whereas salting a hash involves adding a predetermined piece of random data, here the salt often takes the form of a user input such as a password.

---

A salted transformation is reversible if the salt is known, so an attacker with access to both the protected transformed template and the salt is able to revert back to the unprotected template. Consequently, the user of such a system not only needs to provide the salt every time the biometric authentication occurs, but also needs to keep that information secret.\(^{40}\)

The second type of transformation is non-reversible—in biometric jargon, it is “noninvertible.” These are mathematically complex processes of warping the template data onto new shapes using a formula that maps more than one minutia onto the same point. Any given output of such a noninvertible transformation can be derived from a large number of possible inputs. Even if the warped output is compromised, the attacker has no way to work out what the input was. One advantage of this method is that the key used to warp the data does not need to be kept secret, because the computational challenge of reversing the warping by itself serves to protect the stored template.\(^{41}\)

**BIOMETRIC CRYPTOGRAPHY**

Whereas cryptographic techniques have proved valuable in protecting the security of user’s passwords, there are peculiar aspects of biometric authentication that prevent the straightforward use of standard encryption techniques. Traditional cryptography is generally predicated on exactness—a specific key is used to encrypt some data, and an authorized user demonstrates their authorization to access that secured data by using the one and only decryption key. Sometimes the encryption and decryption key are the same (“symmetric cryptography”) and sometimes they are distinct (“asymmetric cryptography”), but generally speaking there should only be one set of keys. Using biometric data to generate or present a key is therefore complicated by the imprecisions inherent in biological traits.

A password can be entered with identical keystrokes every time, ensuring that the encrypted hash of that password is always the same. Biometric data is not so consistent. The inevitable variation between successive templates of the same finger does not impede *matching* because the assumption is that two templates match as long as they are substantially similar—but this variation does pose problems when trying to secure the templates through hashing.


Traditional cryptographic hashing algorithms have a so-called “avalanche effect” whereby a small change in the input snowballs to a significant change in the output. Cryptographic hashes are an ideal way to validate passwords because the correspondence between the user’s input and the stored password is reflected in the correspondence between the hashes of those two items. When looking for mere similarity between two items, hashes only exaggerate the differences and prevent matching.

One alternative is the use of “context triggered piecewise hashes,” more colloquially known as “fuzzy hashes.” As described by Jesse Kornblum in a 2006 paper, a fuzzy hash divides a source input into a series of chunks, and then hashes the chunks individually, concatenating the result into a single string. Consequently, two files that are substantially similar to one another will have fuzzy hashes that substantially match as well.

Error correcting codes have also been used to bridge the divide between biometrics and cryptography. Computers and telecommunication systems commonly employ error correcting codes to protect the integrity of data when transmitted or stored on noisy systems. Although many complex techniques have been developed, they all derive from ideas pioneered by American mathematician Richard Hamming. In the late 1940s, Hamming was working on the Model 5 relay computer using a program with built-in error detection. If it could not read a section of data after three tries, would abort the process. He was allocated time on the machine only on the weekend, so he could initiate his program at 5 pm Friday and return at 8 am Monday to collect the output. When Hamming arrived on Monday morning, he was deflated to find the machine had given up and produced nothing. He reset the system at the end of that week to try again, only to once again find a blank tape upon his return. Exasperated at wasting two weeks, Hamming decided if the machine was smart enough to discover an error, he was going to make it smart enough to fix the error too.

At its root, the idea behind error-correcting is to pad the data with redundant information such that when individual parts of the original information are damaged, there is additional information around it to identify where the error has occurred and provide context for correcting it. “Hamming distance” is a measurement

---

44 See also Garg, "A New Design Approach of Fuzzy Hashing Schemes For Fingerprints" (2015).
of the degree of difference between two data strings. In some systems, error-correcting codes and Hamming distance measurements are used to treat the templates as if their natural biological variances are noise or data corruption to be “corrected.”

Several methods exist to combine error-correction techniques with traditional cryptographic approaches to secure biometric templates. For example, “fuzzy commitment” schemes are similar (and cryptographically related to) hash functions, and “fuzzy vault” schemes allow a vault to be locked and unlocked with keys that are only approximations of one another. These and similar approaches are collectively called “Key Binding” techniques, because they create an encryption key by binding the biometric template to an additional set of so-called “helper data” that is completely independent of the biometric data. The helper data does not expose any significant biometric data but is necessary to extract a viable encryption key. In these systems, the matching is performed indirectly on the extracted key, not the template itself.

A second category of biometric cryptosystems is distinguished by using helper data in a different way altogether. “Key Generation” systems use the biometric template to derive helper data, which is then used to generate a key. These types of systems use the biometric data and helper data to generate two keys—an asymmetric pair of encryption and decryption keys. The encryption key is used to encrypt the sensitive biometric data for storage. The decryption key is then encoded using the biometric identifier, and this encoded decryption key is stored along with the encrypted template. The original unencoded decryption key is stored separately, without the biometric data. The encryption key and the generator used to create it are destroyed and not stored at all. When the subject attempts to authenticate themselves into the system, the incoming biometric data is used to extract and reconstruct the decryption key, which can then be used to decrypt the biometric template. The security of such a system is based in part on the separation of the components. If the decryption key is compromised, the encrypted data is protected because it is separate and distinct. If the encrypted data is compromised, it is protected because without the subject’s biometrics it cannot be unlocked.

---

HILL-CLIMBING AND SPOOFING

The preceding discussion highlighted notable technologies that are commonly used to protect the storage of the templates on the back-end of the system. The purpose behind the various encryption and transformation techniques described above is to protect the security of the biometric template by, in essence, keeping it out of play in the first place. A transformed and/or encrypted template is a sequence of binary data that was created from a biometric template but is itself something else. If a protected template is compromised, accessed by an unauthorized intruder, it is designed not to be reversible back to original biometrics. In the event that fraudulent or fake credentials are presented at the front-end sensor side of the system, additional hardware and/or software based countermeasures may be used to address the spoofing threat.

Brute force attacks take on a different character in the realm of biometrics. When brute forcing a password, for example, the all-or-nothing threshold by which hashes can match means each individual trial is its own discrete event. When brute forcing a biometric template, however, the goal is to reach a near enough match, so each trial returns a certain degree of feedback that can reduce the entropy for the next attempt. This is called “hill climbing,” and assumes the attacker has gained some access to the output of the matcher module and can use the similarity score to tweak the next input. Each successive input is iteratively adjusted and resubmitted, over and over, to improve the matching score until one works. To guard against this kind of attack, a system may employ a lock-out mechanism after a specified number of unsuccessful tries.50

While reverse engineering a synthetic fingerprint from a protected template is complicated at many stages by steep mathematical challenges, there are far simpler means by which an attacker can obtain a person’s fingerprints. The entire science of fingerprint identification emerged from the observation that people leave their fingerprints on almost everything they touch as a matter of course. Obtaining copies of latent fingerprints left behind on various surfaces is relatively easy. In some cases, subjects might be co-opted into allowing molds of their fingerprints to be taken. There are also ghoulish possibilities of attackers attempting to use severed fingers.

To guard against such situations, sensors can include “liveness” detectors. Real human fingers perspire, for example, and the person holding their finger against the sensor varies the pressure and orientation as they do so. Some sensors are designed to take several template samples over a period of several seconds to pick up these subtle variations, which artificial fingers will not have.

A widely publicized recent incident in Michigan serves as an illustration of these technologies in use, and the degree of difficulty they pose to unauthorized users

---

attempting to gain access to a biometrically-sealed account. In the summer of 2016, police in Lansing found themselves in a technological dead end on a murder case. They suspected that critical evidence regarding the crime might be on the victim’s phone. The Samsung Galaxy S6 in question was locked with a fingerprint, but the investigators did not have access to the dead man’s fingers. The detectives turned to Michigan State University for advice on how to bypass the security, only to be told by Detective Andrew Rathbun of the MSU Police Department’s Digital Forensics and Cyber Crime Unit that no technology exists to bypass the fingerprint security on smartphones. As an alternative, the police next contacted MSU’s Professor Anil Jain, one of the scientists who in 2007 demonstrated the ability to create a synthetic fingerprint from minutia coordinates. Because the victim had been previously arrested, his fingerprints were already on file. Jain created 2-D and 3-D replicas of all 10 of the inked fingerprint images held by law enforcement, but none of these 20 copies unlocked the phone.

A post-doctoral scholar working on Jain’s team, Kai Cao, then developed a custom software program to digitally enhance the reconstructed fingerprints to refine their quality and repair discrepancies that existed in the ink copies taken during the subject’s arrest. These were then printed with an electrically conductive ink to give the artificial finger the same conductivity as a living one, to fool the sensor’s liveness detector. This attempt succeeded in unlocking the phone.51

Jain’s team had the advantages of working from a complete set of inked fingerprints taken under controlled conditions by professionals, provided to one of the elite researchers in the field, with the full resources of a public research university with a dedicated Biometrics Research Group,52 and yet only succeeded after dozens of failed attempts. Had the phone been configured to automatically time out after a set number of consecutive failures, or used more complex liveness detection, the outcome could have been very different. It is also unclear whether the replica fingerprint that Jain’s team engineered would be successful if used in another system.

CONCLUSION

In 2012, the United Kingdom’s Prince William began a stint as a Search and Rescue helicopter pilot in the Royal Air Force. The Royal Family deployed an official Ministry of Defense photographer to take pictures of the Prince at work. After approval by Buckingham Palace’s public relations team, a selection of pictures were distributed to the press, and posted to a website dedicated to the lives of the Duke and Duchess of Cambridge. Only after the photos were published, however, did anyone notice that

52 See http://biometrics.cse.msu.edu/.
they included various defense department passwords printed on various papers posted in the background of several photos. 53

The situation was a striking security lapse, but the public relations debacle that ensued was mostly treated as an occasion for gentle mockery, not opprobrium. Prince William is an intelligent, well-educated, resourceful man backed up by a team of handlers. He saw nothing wrong on that day, nor did the other soldiers and staffers who routinely worked in that office, nor did the approved photographer, the Royal Family’s media relations staff, or any of the editors or publishers who proceeded to make these photographs available to the public at a national and even international scale. The number of gatekeepers who let this slide is extensive.

People choose terrible passwords, if they can even be bothered to update the default password in the first place, and then write them down and sometimes print them in the newspaper for all to see. Phishing agents easily persuade people to give their passwords away to strangers, and when all else fails the brute force attacks rarely need to try anything beyond “123456.” The website HaveIBeenPwned.com publishes an online directory of over 551 million user passwords that have been exposed in data breaches, and should therefore be discontinued. 54 Strikingly, the passwords in this directory appear on average in six different data breaches—and some appear thousands of times. In other words, users get their passwords exposed, and then that exposure snowballs because they have reused that password in multiple other places. In short, the human factor makes password security inherently vulnerable, and a single exposure has the potential to escalate liability for that user and others connected to them.

Biometric-based security solves many of those problems, and re-integrates the process of authentication back with the subject’s actual identity. Instead of depending on the good behavior of any individual user, most biometric security measures are technological in nature and apply generally to the system at the sensor and/or database level. There are meaningful threats to the security of a biometric system, and ongoing improvements to biometric security can mitigate these risks but may never wholly defeat them. That being said, the greatest risk in a biometric authentication environment comes from the possibility of unauthorized access. A successful hill-climbing attack, for example, can allow an unauthorized user into a system. Whereas a breached password may represent an escalating exposure risk, a compromised biometric system is likely to be limited to that system alone. Because of the differences between templates and template systems in different applications, a stolen template from one environment is likely useless anywhere else. Protected templates are supposed to be designed so that they cannot be reverse engineered to original biometric data. Although determined attackers might be able to replicate or synthesize fake fingerprints, that

54 https://haveibeenpwned.com/Passwords.
possibility is both exceedingly challenging (as the Lansing Police will be the first to tell you), and also is a risk that exists independent of the security protections placed on biometric templates.

The catchy phrase “you can change your password but you can’t change your face, or your fingerprints” remains a useful reminder to those involved in biometric security that there are meaningful privacy and security concerns that deserve serious and ongoing attention. However, users of such systems can take comfort in the fact that the analogy only goes so far. Password-based security is so poor, people are accustomed to having to change compromised passwords, but the scenario in which a person would need to change their face or fingerprints remains in the realm of speculative fiction.