Songs like "The Look of Love," "The Tracks of My Tears," "The Shadow of Your Smile," and "The Way You Look Tonight" show how bio-identification expresses our deepest emotions. Cats and dogs also use sight and smell to identify the people they trust. Biometric identification is the most natural strategy developed by humans and other animals.

In addition, by time of this writing, humankind has developed machines that are better than people at searching enormous lists, categorizing traits and making comparisons. And in other branches of scientific endeavor, we have learned to easily isolate biometric measurements that are nearly impossible to spoof and measurements like DNA that are conclusively indicative of a person’s identity.

So why are biometrics not the primary method, or the only method, that our society uses to identify humans for business and governmental reasons? Our quotidian transactions are dominated by PINs, passwords and identification cards issued by trusted authorities, rather than a measurement of who we really are.

Part of the reason is founded in history and technology. The technology used to accept cards, magnetic stripes, microchips and the machines that capture memorized numbers have been trustworthy for decades, while the technology used to measure and compare our physical beings is only now beginning to be trusted. Plus, as we discuss in more detail below, people have been naturally adverse to machines that read their physical natures. This method is somehow too precise and undeniably creepy, and when organized poorly, biometric readers create a database of personal traits that may be abused by the database’s holder or stolen by people of evil intent.

But we may have recently turned a corner in the use of biometrics for day-to-day identification. Technology is now strong enough to read our physical traits and make useful comparisons and distinctions. Cryptographic storage methods have eliminated the problem of raw, unalterable physical data stored...
that can be connected back to the subject. The devastating data theft at Equifax in 2017 is likely to accelerate use of biometric identification for security and account identification by highlighting the inadequacy and risk of using social security numbers for commercial transactions.

The past four decades of biometric security applications have demonstrated both strengths in these systems and problems in their design and application. This paper uses some of this knowledge to assist legislators, regulators and business executives who are considering how to manage and limit biometric systems. Biometric readings raise legitimate fear in many policymakers: fear of government or business overreach, fear of criminal misuse, and fear of dehumanizing treatment. Mistakes in applying biometric tools have also led to avoidable problems. We discuss the risks and rewards below, pierce some of the mythology around bio-identification, analyze current attempts to regulate the technology, and propose a measured way of thinking about how biometrics affect individuals and society.
What Are Biometric Readings and Why Are They Significant?

Biometrics is the measurement of physical traits and behaviors. The field is used to identify individuals by measuring a physical characteristic and comparing it to a previous measurement. The features measured can be publically available, like faces and voices, or hidden from plain view and only readable by machine, like retinas and vein patterns. Or they can be both easily seen and hard to visually measure or compare, like hand geometry or iris patterns. The measurements can be as general as body type comparisons, and as specific as DNA matching.

A. How do we choose a trait to measure?

Certain human physical and behavioral traits work to distinguish one person from another, while others do not do so well. When you leave your car in an enormous mall or stadium parking lot, it doesn’t make sense to try to remember your location by the cars that have parked around you because some or all of those cars will be gone by the time you come back. The pattern of other cars demonstrates a failure of permanence. You would be better off counting the number of rows or remembering the specific light post you parked under; for the purpose of your memory, those things will remain the same for the entire time you are parked.

Similarly, in biometrics, there are some traits that lend themselves best to measurement and comparison. Those traits have the following attributes.

I. Permanence. Like the parking example, a biometric measurement used for practical purposes should be a trait that generally doesn’t change over time. Fingerprints, hand geometry, iris patterns, vein patterns beneath skin, and even face and voice remain the same in important ways over a lifetime. Of course certain traumatic events and diseases can change a person’s physical being, but these occurrences are rare enough not to be a major consideration into what trait to measure.

II. Universality. A measurable trait used for practical purposes must occur in so much of the relevant population that it can be measured and compared in almost anyone. Mole patterns may be unique on human faces, but many people simply do not have moles or other features on their faces, so mole geometry would be a poor choice to build a biometric measurement system. Nearly everyone has a measurable face and fingerprints, which makes these traits better for the task.

III. Uniqueness. The trait measured for biometric systems should vary enough in every person so that it can be used to distinguish one from the other. Generally, if you choose a trait that takes a very close and specific measurement of any human body, you would find an adequate sample of uniqueness to verify that one person is different from another based on that measurement.

IV. Measurability. How difficult is a particular biometric trait to capture and quantify? Can we do so with enough detail to distinguish small difference between people? Do we have a machine that can do so cost
effectively? Can the subject measure herself, like with a selfie, voiceprint or fingerprint on a smartphone, or, in the case of passive biometrics, can we measure the behavior without the subject knowing about it? All of these questions are important to practical matter of implementing a biometric system.

V. Acceptability. If your method to measure and differentiate people involves poking the subject in the eye or piercing his skin to collect blood, then don’t be surprised that no one wants to participate. A biometric system should be easy enough for subjects to submit their measuring trait without pain, discomfort or embarrassing disclosure. It may be true that every person’s navel is different, but gathering navel data would be difficult, embarrassing for some, and many would refuse to offer their navel for measurement. Some people refuse to place a finger or hand on a pad used by other people for fear of catching a disease. Remote capture always seems to be the most acceptable method. But if you require merchants or consumers to purchase and either install or carry a $3,000 set of sensors to manage your biometric measurement system, then they will again refuse to accept your system.

Some other factors can matter as well. How easy will it be to circumvent your biometric system? If you can simply record someone’s voice and then play it back to present yourself as the person whose voice you recorded, then the voice pattern system will not work well enough. Also, the system must perform well and efficiently for the chosen application. As we discuss below, some systems like face recognition, voiceprint analysis, and keystroke patterns work well remotely and can even be used without the knowledge of the subject. Other systems, like hand geometry and retina scanning can work well when the subject presents herself in person and is standing in front of the measuring machine and its operator.

B. How are the measurements used?

I. Identity Capture and Verification. One of the primary problems of our age-of-convenience is identifying people who should be authorized to enter a building, receive treatment under certain health insurance, or access a financial or shopping account. We expect companies and governments to restrict access to our personal accounts so that only one person can reach them, and we expect to do this over the internet from a computer device a thousand miles away from where the account is housed. We need to distinguish people who want to enter a building or access an account from the people who should be permitted to do these things, and we need to do so when an authorized person may not be available to make distinctions or when the person seeking access is not standing in front of us.

Traditional security practice dictates that an account holder identify herself through one or more verification factors, including (1) something you know (like PIN and password), (2) something you have (like an ATM card or a security token), or (3) something you are (which can be satisfied by biometric comparisons, including your signature). A century ago, signature and official seal or stamp provided proof of identity, along with a physical presence that other people could see and hear. Recently, remote access removes the requirement (and the assurance) of a physical presence, and so the first two factors—a card and a password—have served as promise of identity. For larger and more important accounts, another indicator of knowledge, a person's social security number, provided additional assurance.
The card and password system which worked for decades seems to be breaking down for many transactions, and the theft of tens of millions of social security numbers in the past five years has led banks and retailers to search for a different method of distance verification. Biometrics can be used to fill this gap. Many banks are currently using voice pattern recognition to add a layer of assurance to telephone-originated transactions. Disney required hand geometry measurements for repeat visits to its theme parks. Retailers in South America installed a system that accepts selfies taken at checkout as a facial recognition check on identity to help pay for purchases. With some obvious limitations and risk of false negatives, it is likely that consumer biometric security is a growing industry as the systems reduce in price and as technology is socialized into consumer society.

Biometric systems are used for workers, both in measuring attendance and in limiting access to secure areas. Frequent travelers register fingerprints and hand geometry to reduce airport waits. Schools are using facial recognition programs to keep attendance and safety under control. Hospitals keep track of surgical patients with biometric systems. The US military records faces and even DNA of people in occupied zones to differentiate enemy combatants from the rest of the population.

II. Authorization. Some of the examples above—access to secured areas, account holder recognition—involves authorization as well as identification. Authorizing takes authenticating one step further, recognizing not only a person but the status of that person, and then granting the person the privileges of his status. That privilege could simply mean access to the janitor’s closet, or it could provide entry into a multi-million Euro Swiss bank account. Authorization is an excellent application for biometric systems, which can provide a higher level of certainty than other security factors.

We are most familiar with consumer verification that allows us to access credit balances, checking or investment accounts, and our Amazon Prime membership. The commercial gatekeepers not only need to some indication of who we are when we try to access these accounts, but they need to know whether this person still holds the right to remove money or to order the latest super hero movie at a discount. The airline must confirm that our flight is credited to the correct frequent flier program. The gym checks to learn if you have continued to pay your membership fees. While many of these applications are low money risks, and therefore managed with PIN and password, more apps are using Apple’s fingerprint or facial scan measurements to confirm account or membership verification. Vocal patterns are becoming inexpensive and precise enough to use for customers accessing accounts over the telephone.

Equally important are verification reviews that are tied to employment. Some are spatial—who is allowed in the restaurant kitchen, the tower elevators, the airport baggage handling zone or the hospital operating room? We need to know the person and we need to know that the person is still employed in a job that could gain access to these spaces. As with consumers, some are account-centric, where only the president or chief financial officer of a company may access the corporate accounts, or only the members of the chemical research team can see the latest lab results. Some are electronic as more of our important business information moves onto the web. But employment-related
Some companies use biometrics to provide more accurate records of employee attendance and participation in training exercises and other functions.

III. Record Keeping. Some companies use biometric identifiers for record keeping. Beyond mere verification and authorization, these businesses rely on the thumbprint scan to record when a worker entered the factory in the morning and when she left it at night, so that her biweekly paycheck can accurately reflect time spent on the job. Similarly, people are often biometrically registered for important training exercises, so that their employer can prove that each person received the required training hours. Transportation companies use biometrics not only to locate people and packages, but to log the miles spent and the time taken to arrive at a destination. A broad range of biometric measurements, from keystroke patterns to gate recognition, may be used for recordkeeping functions.

IV. Law Enforcement and Military Applications. A common procedure of body science is the reverse of the above-described methods. Where consumers and employees activate a one-to-one measurement to determine if a specific person is allowed into a place or an account (known by the biometric industry term of art “Verification”), many organizations process biometrics in a one-out-of-many measurement to discover whether a particular capture of a single face or single fingerprint matches anything in the organization’s database (known by the biometric industry term of art “Authentication”). Criminal investigation is one of the earliest uses of biometrics (see the 1870s Rogues Gallery of New York Police Inspector Thomas Byrnes as a population to authenticate an arrest) and the ones most prevalent on police procedural television shows. When the Las Vegas police investigate a murder, they send the accumulated information to the crime lab, where the brilliant and intrepid CSI draws out identifying features like fingerprints and hair or skin samples. These may be used to identify the victim or the perpetrator, but in any case, a biometric reading is often the best evidence that someone was at a particular crime scene. And biometrics for law enforcement keep advancing. For example, on July 17, 2017, Motorola announced that it is working with an artificial intelligence software startup, Neurala, Inc., to develop facial recognition programs that can be used in police body cameras. When installed, local law enforcement can quickly and accurately check if a driver owns the car he is in, and if he should be treated as a dangerous criminal.

While often not given great weight because it is circumstantial evidence, biometric clues left at a crime scene can be much more accurately damning than direct, eyewitness testimony (which can be simply another form of biometric identification). The recent application of DNA comparisons has allowed law enforcement officers and prosecuting attorneys to feel more certain in their accusations, although as we learned by the FBI’s mistakes in using DNA evidence in the Madrid train bombing case in 2004, the precision of DNA comparisons can also lead to a false sense of certainty. In these cases, a single or multiple items of biometric capture, from video to blood samples, is either compared to a broad database to pinpoint the person who left the biometric sample or compared to a pool of criminal suspects who might have been at the scene.
And finally, a military practice of biometric measurement allows groups like the US Army to establish a baseline identity for each person they find in a particular war zone, so that the soldiers can better determine if a captured person or a local homeowner is a friend, an enemy, or an innocent bystander caught in a cross-fire. Military units in Iraq and Afghanistan have found that keeping biometric records of the local populations allows more accurate determinations of friendly and hostile people. Extensive use of biometrics in the Afghan war has helped the US and its allies’ military forces separate insurgent forces from the indigenous population. The US military currently uses three primary devices for collecting the bulk of the biometric data harvested in Afghanistan including the Secure Electronic Enrollment Kit (SEEK) which used now by special operations forces. The SEEK is a handheld device capable of taking fingerprints, scanning irises and snapping photographs. It also has a built-in keyboard for remotely entering biographical information on the subject.

C. Why regulate biometrics?

Many US consumers fear the pervasive use of biometrics in our everyday commercial life. Some have practical concerns with the health risks of touching common public measuring devices or the fact that defeating a biometric reading machine may be easier than it seems while a positive match implies an unwarranted certainty. In addition, many people are anxious about data security risks that may arise if an organization holding your biometric identifier is hacked, so that criminals can now present themselves as though they were you. The unchangeability of physical characteristics like fingerprints or iris patterns makes this apprehension deeply troubling to many people. Some are concerned that use of certain biometric measurements for access into financial accounts or critical infrastructure zones will encourage violence, as criminals or terrorists find it easier to remove the measured finger, hand or eye of the authorized person than find a more clever way to defeat a biometrically activated system. Below we examine reasons why the thoughtful implementation of biometric access systems can easily avoid most of these problems.

Of course, some people are simply worried relinquishing control of their intimate data. They believe that the company or government agency that captures and holds your biometric information could turn the information against you someday, perhaps denying insurance coverage or employment based on the data.

Some people are worried that the company or government agency that captures your biometric information could turn it against you someday, perhaps denying insurance coverage or employment based on the data.
against you, as the Jewish population of the Netherlands learned when their government’s detailed personal records, which were used for distribution of benefits, were suddenly turned against the people when the Nazi’s forcibly took power. If the holder of your biometric data were inclined to punish its political enemies, none of the data subjects would be safe.

Another area of legitimate concern is how the general public might use biometric programs if everyone had access to them. For example, an early Google facial recognition search tool was quickly pulled from public access. The tool worked too well, allowing someone to find recent pictures of a person no matter how much the subject had changed with age. This was problematic for people who did not wish to be found like women who have moved away to hide from their abusive partners or spouses and people in the Federal witness protection program. A searcher could use the high school yearbook photo of the person he wanted to find, and run the Google program to find later pictures of that person on the web. Some biometric tools may be too accurate to share with people who might use them irresponsibly or maliciously.

Any of these fears might underlie a bill to regulate biometrics. Many biometric regulations have been introduced in state legislatures, and several have been enacted into law. These laws are varied and based on different assumptions. Some are targeted at protecting children. A child might be forced to provide a non-public biometric measurement that could haunt her later in life. In addition, to hold a biometric reading describing a person is to hold power over that person, and some legislators have been concerned about giving companies and non-parent individuals too much power over other people’s children.

Most of the regulations show an interest in protecting consumers from corporations. In this age of the internet, some companies collect enormous transactional and behavioral data about their customers or service users. Adding biometric information to this mix could make consumers identifiable by the companies in nearly every situation, which many would consider a significant infringement on the consumer’s privacy. Biometric data could be used to track people. And, as demonstrated above, biometric databases may be breached and the information stolen, granting criminals or hostile governments an ability to make mischief with the personal physical traits of anyone in the database.

Some of the bills come from a different direction, not limiting the capture and processing of biometric data by companies, but limiting biometric capture and storage by government entities. For people who are concerned with the power and coercion of the government, keeping biometric out of government hands is an important protection for a free population, and they do not want people forced to give up their private biometric data to government control. Many of these bills and regulations have been directed toward limiting public schools from capturing children’s biometric readings and using them as standard identifiers and record keeping systems in public schools. It is interesting to note that despite the fact that law enforcement (including the national security apparatus) is by far the largest collector of biometric data and holds many of the most critical biometric databases, including fingerprints, faces and even DNA, very few of the proposed legislative actions would have any effect on police forces or the FBI. Legislatures seem content to allow this biometric aggregation to continue, even if they look to curtail the capture of biometric readings by other arms of the government.
D. Important Legal Distinctions

When considering the application or the regulation of biometric capture, whatever the underlying reason, executives and legislators should carefully consider several important factors of biometric measurements that can have legal and practical significance. These factors make a difference in how biometric readings are used and how they can be protected. Regulators ignoring these factors are unlikely to achieve their goals.

I. Public Biometric Capture vs. Private Biometric Capture. As noted above, some physical traits about people are as plain as the noses on their faces. In fact, measuring the nose and its relationship to the rest of its adjacent facial features is a commonly used biometric. But the face, as well as the voice, the gait, and the general shape of the body are public biometrics. These are features that we all offer to the general public every time we walk out the front door. People have always used faces and voices to identify people, and probably always will. So such public biometric offerings in some ways need less protection from the government than other, harder to see and capture biometric readings. In other words, if a bad person hacks into a database and steals an entire set of facial recognition files, including yours, that person really hasn’t taken anything that he could not have received anyway by just waiting for you, and the others in the database, to walk outside or to show up in a store or office lobby. Grabbing an entire database of these pictures may be somewhat concerning, but we can always check someone’s public biometric (face, for example) against the one we know from many other contexts.

Conversely if the local airport has a database of retinal scans, and a bad person hacks in and steals all of these biometric files, people are likely to be more concerned. The biometric subjects would have submitted themselves to a special scanning machine to capture the patterns in their retinas. And the database thief could use these scans to enter sensitive areas of the airport. Stealing hidden or private biometrics is more of an imposition and violation of the subject’s privacy. This is something about the data subject that no one but the biometric database holder knows. Not even your mother or probably your doctor knows what your retina looks like and how it is different from the retinas of your neighbors. Private biometrics like vein patterns are in many ways more sensitive than their public counterparts, and this difference may affect the way that each type of biometric capture is described and regulated. Some limitations on capture, storage and use may be appropriate for hidden biometric measurements, whereas similar regulations of facial capture could be so overbroad as to affect standard company and government video surveillance.

Certain important biometric measurements are effectively private, although they may be captured in very public ways. For example, while our fingerprints are available to the public, they are not perceptible by the human eye, so we don’t think of them as public. That could be changing as new photography and software allows accurate fingerprint capture from distances as far as fifty feet away. However, this new technology is unlikely to affect our perception that fingerprints are a biological measurement that we can refuse to offer to the police or to an interested business. We can leave them on the table or coffee cup, but we have the right to refuse to do either one.

Similarly, DNA is a highly sensitive biometric measure. DNA is the basis of our lives, it is unique to each person, and it can provide deep, important,
private and actionable information about us to people who might use that against us. In most situations, US citizens would need to consent to allowing law enforcement to take a sample of our DNA. But each of us is constantly sloughing off skin, hair and fluids that contain our DNA and could be used to capture and measure that biometric information. We think of DNA as the most private of all biological markers, but we leave samples of it everywhere we go. Drink from a cup, you left DNA on it. Brush your hair, your DNA is on the brush. Cough into a tissue and throw it away, your DNA is likely in the trashcan. Even more than fingerprints, US law recognizes the importance and fundamental privacy of a person’s genetic code, even if that code can be casually collected by others.

II. Physical Biometrics vs. Behavioral Biometrics. The biometric measurements that we most often discuss are physical aspects of our corporeal selves. In other words, parts of our body. Faces, fingers, hands, eyes and navels are all unique to an individual, essentially unchanging and can all be measured and used for identification. Of course serious trauma like losing two fingers will change the geometry of your hand, but your hand is not like your hair, which is frequently cut and can be worn in any number of styles. Your fingerprints will likely always be the same fingerprints. Your voice is even considered a physical characteristic as it is a result of the unique vocal structure and mouth size contained in your head and neck, but your speech pattern is a separate behavioral biometric to be measured. Voice depth may change over time, but many aspects of both voice and speech patterns remain consistent.

But there are other biometric indicators that we have used to identify people for centuries, and these are known as behavioral traits. These include how you sign your name, how you type on a keyboard, and even how you walk into a room. People have demanded signature on a document as a biometric identifier since writing became commonplace, and in the 1860s telegraph operators could tell which person was sending a message from the speed and manner that the dots and dashes were entered. Today’s most common behavioral biometrics reflect the technologies that we enlist to remotely access accounts: keystrokes, speech patterns, the amount of pressure in pushing smartphone keys, the angle a smartphone is held when information is entered. All of these biometric measurements use the manner of technical communications and the input mechanisms that can be measured.

As a solution to current problems, behavioral biometrics are often used to supplement a series of measurements taken to identify someone attempting remote access to an account. If a bank uses a combination of four or five behavioral characteristics to verify a remote account holder, then it has more certainty that the proper account user is identified, and less chance that a hacker or thief would even try to mimic all of the biometric characteristics. Using gummy bears to capture a finger print is relatively simple compared to the need to correctly mimic multiple behaviors in a careful enough manner to fool the measuring computers. In addition, the more the same account holder enters her account remotely, the more accurate calculations can be to pinpoint her biometric measurements. This means that a company using this method of verification can be more certain of its authorizations over time.

III. Active Entry vs. Passive Entry. Biometric identification works by comparing the current biometric measurement against past
measurements and acknowledging the correct identification if the measurements fall within a pre-determined margin of error. For this system to work, it must collect initial measurements of whatever biometric trait is at issue. This process is called enrollment and it can happen in different ways. Active biometric capture requires a person to actively and knowingly participate in providing the initial samples to be measured by the system. For example, active enrollment for voice systems involves the user reciting several specific phrases that will serve as the basis for his voiceprint. Active fingerprint verification systems like those on earlier versions of the iPhone require the phone owner to enter many angles of the same fingerprint so that the system can make the most accurate capture possible. These systems have advantages as the knowing and directed entry of data can allow a more sensitive positive identification with less mathematical margin of error.

However, some systems accept initial enrollment passively. For a voice system, this means that the technology would measure vocal tones from a normal conversation of the measurement subject, rather than making that subject speak specifically-defined phrases. Passive biometrics can be instituted without the subject knowing that she entered biometric data into the system. Passive systems often use various behavioral biometric reading, but can also be managed using voiceprint, iris or facial recognition software. Passive biometric capture may be attempted at a distance with cameras and/or microphones, or may use input devices operated by the measurement subject.

Passive enrollment can have advantages in obscurity—the system is measuring characteristics that no one knows are being used for verification. Not only is it difficult for hackers to game a system where they may not know what biometrics are being measured, but the company sponsoring the system could add new measurements to the mix at any time without notifying anyone about it. Some people worry that it is an invasion of privacy and a dehumanizing aspect of current security to take someone’s biometric measurements without the subject’s knowledge, but many businesses feel the added security by obscurity is worth the risk.

Using passive biometric regimes can also allow continuous verification, where the monitoring company uses keystrokes, video, pressure readings, gyroscopic measurements, and/or the smartphone accelerometer to keep monitoring and comparing biometric readings during the entire session in which the subject interfaces with the interested company. This type of continuous verifications works especially well in a remote testing context, where it is important that the person who signs onto the testing site is the same person who actually answers all of the questions.

**IV. Samples Stored Intact vs. Samples Converted to Non-Reversible Reference Template.** One of the most important distinctions for the privacy and security of biometric databases is whether biometric comparison samples are stored as a clear picture or stored in a manner that obfuscates the sample so that it cannot be productively used by anyone who steals the sample. If they are stored as a clear picture, then that database is vulnerable to hacking and to reapplication of the biometric pictures held in the database. A hacked database with clear pictures can be turned around and used to break the database holder’s security, or it can be dumped into a larger file on each of the biometric subjects to use anytime the hacker wants to pose as the particular
person whose biometric picture he holds. Clearly, this is a dangerous situation, but storing biometric readings this way is not necessary and is not a best practice in the security industry.

Instead, the biometric samples can be converted into reference templates that can only be read by the specific program that created them, and can only be read as initial comparative files and not successfully submitted as hashed later samples used for account or room access. If these reference templates are created using appropriate cryptography, then they cannot be reverse engineered to create biometric picture file. Storing biometric data as non-reversible reference templates should relieve much of the general public’s unease with biometric systems. In this method of storage, a thief should not be able to steal and successfully offer your thumbprint or iris scan to mimic you for any biometric security system. Even if the hacker breaks into the database and steals all of the reference files, the files will be unusable and the hacker will be left with nothing more than a drive full of math problems. For this reason, legislators and regulators should consider requiring non-reversible reference template storage for any biometric systems, and businesses should not settle for a biometric security network that stores its samples in a reusable fashion.

**V. False Positives and False Negatives.** Every system and every important decision should involve, tacitly or explicitly, a determination of which side would be most costly to err in favor of. Consider when you are deciding on your dinner order at a restaurant: you tacitly think about whether you would prefer overeating or undereating at this meal. You will try to hold the balance, but if undereating is your concern then the steak and potatoes will be more appropriate. If you are worried about overeating then ordering salad or just an appetizer may be the best idea. These bilateral distinctions between too much and too little comprise the core of management for biometric decisions, and, like your dinner decision, the correct answer will depend on circumstance.

In biometric systems, the bilateral decision is between false positives and false negatives. If the system is calibrated too tightly and a tiny margin of error is all that the system administrator will accept, then the company should expect to see many false negatives, as people who present their biometric reading for comparison are rejected because the new sample does not match the reference template. Erring on this side of the equation would be acceptable, and even advisable, in systems where it is very important that only authorized people are allowed into a restricted area or if ten million dollars was at stake in each account admittance decision. Better to keep the right people out in these circumstances than allow the wrong people to gain access. In systems where there is much at stake, you can always send people down to the access point and force the data subject to offer up different proof of his identity and authority. And people are unlikely to quit their jobs or avoid your security when so much is on the line.

Conversely, if the stakes are low and the volume is high, the system administrator may prefer to set a more flexible comparison with a high margin of error, so that people who match the reference template are generally given the benefit of the doubt and allowed to access the system. This choice might be the best method of encouraging the use of consumer biometrics at retail stores out here in the physical world. First, it is unlikely that a thief or hacker would waste the many hours it would take to break the biometric code and to pose as a different person for
the use of her credit card. Credit cards today have a limited shelf life and since the banks are vigilant and using artificial intelligence programs to seek out unauthorized card use, a thief could probably not benefit more than $500 or so before the ruse was shut down. The (stolen) prize is not worth the (illegal) effort.

But on the other side of the equation, a consumer has very little patience for using a payment method that frequently hiccups and doesn’t easily allow the user to pay for items at a restaurant, hotel or store. If a consumer reaches the register with a screeching toddler and a line of six people pressing behind him, he will have no patience for a system that is set so tightly that it usually rejects verification—telling him that his thumb is not actually his thumb for the purposes of payment. He will quickly move to another mode of payment and never come back to the original difficult method. So it would be smarter to err a little more on the side of false positives, where a bad person might game the system for a short time and a small reward, then it would be to allow many false negatives and lose the support of people who use the system.

Every biometric security system presents precisely this problem, calibrate it too tightly and you receive more false negatives creating frustration for the users but deeper security to protect targets. Calibrate it too loosely and keep the data subjects happy, but run a greater risk of false positives where the system verifies someone who doesn’t deserve it.

VI. Samples Stored and Read in Central Location vs. Sample Stored and Read on Multiple Mobile Media. One other dichotomy in the management of biometric verification systems may have significant legal and practical implications. Many biometric systems capture the biometric measurement and transport it back to a central database where the sample can be compared to the reference template of an account holder. This option for managing access works particularly well for remote access to centralized accounts and for high-value targets where the system is limiting access to a few authorized people. It is easier to protect all of the reference templates in a centralized place and most biometric system administrators see no reason to organize their access management tools any differently.

However, sometimes it makes sense to both capture and store the reference template remotely so that the subject has all he needs to activate the system on his own equipment and may not even be attached to the internet to be confirmed in the biometric system. A perfect example of this type of biometric management is the fingerprint hardware unlock system on the Apple iPhones 6 through 9. The fingerprint reader is right on the front of the iPhone, so the subject is always carrying it with her and does not need to travel to a specific location to be photographed or otherwise measured. The fingerprint reference template may be backed up in some Apple server farm, but it also seems to exist right on the phone itself, so that a subject can open hardware access to an iPhone entirely with equipment and information contained on the phone. This method makes each reference template more vulnerable by itself, but likely makes the entire population of reference template less vulnerable as a hacker could not simply grab one central database to capture all the reference templates.
How Are Governments Currently Regulating Biometric Capture?

Governments throughout the developed world are regulating biometric security and the capture, storage and comparison of the physical and behavioral traits of individual citizens. As described below, the governments of the European Union Member States and of Canada view biometrics differently than the state and federal governments of the United States. While most governments addressing the issue seem to agree that certain individuals need to be protected from certain organizations, the similarities stop there. Who should be protected from whom, and how those protections are managed and enforced, are entirely different matters in different jurisdictions.

Current law is a patchwork of restrictions that often display a misunderstanding of biometric comparison technology and the level of risk it presents to the average person in a developed nation. Current law neither provides comprehensive protection for individuals, nor encourages the application of biometric technology to important security problems. Very few of the biometric protection regimes currently on the books or promoted through regulatory enforcement demonstrate an awareness of the legally significant dichotomies raised in the management of biometric systems. We hope that this paper can help to educate lawmakers so that better analysis will lead to better laws.

A. Protecting Sensitive Information as a Human Right

The Member States of the EU and Canada, as well as numerous smaller, developed nations, protect privacy as a fundamental human right. Defined categories of personal data belong exclusively to the subject individual that each category of data describes. That data subject may decide how such information is used by business and governments, and when such data must be destroyed by the organizations holding it.

These jurisdictions have developed a large bureaucracy to protect these rights, and they can bring enforcement actions on findings that a company is not meeting its privacy obligations. They have instituted the right in government to impose crippling fines on businesses that do not comply with their intricate rules as defined and interpreted by their privacy-centric courts and administrative judges.

Biometric information is classified as a “special category of personal data” in the EU. Applicable laws restrict when a business can capture biometric data, what the business can do with the data once it has been collected, and how long the business is allowed to hold such biometric information. Canada law similarly restricts the use of biometrics; Canada’s privacy regulator, the Office of the Privacy Commissioner, has published the following statement: “Organizations should always seek explicit consent to collect biometric information and give individuals the choice not to use their biometric information for identification or authentication purposes when there are reasonable alternatives.”1

Both the EU and Canada have written their laws to disfavor biometric data collection, with the Supreme Court of Canada holding that biometric security is a potentially privacy-invasive measure. This court provided a test for when collection of biometric readings may be implemented and applied to Canadian citizens, stating that before implementing such a measure, a business must answer four questions.

1. Is the measure demonstrably necessary to meet a specific need?
2. Is it likely to be effective in meeting that need?
3. Would the loss of privacy be proportionate to the benefit gained?
4. Is there a less privacy invasive way of achieving the same end?

This test was used in 2008 to invalidate the use of a thumbprint biometric reading as identity verification and security for taking standardized tests for admission to law schools. According to the Canada regulator:

[The test helped clarify the issues in a complaint about the Law School Admission Council’s practice of collecting thumbprints of people writing a standardized admission test for law schools. The council said the collection aimed to deter cheaters who hoped to slip in substitute test writers. We concluded, however, that a thumb stamp was not essential for authenticating the identity of test writers, and not effective in the way it was being used. This resulted in a disproportionate invasion of privacy.]

The Canadian Supreme Court has yet to define what situations would warrant the use of biometric security and identity verification, but it clearly disfavors the practice as an infringement on personal privacy of Canadian citizens. Canada endorses and the EU requires a business strategy called “Privacy by Design”, whereby the ultimate protection of a citizen’s private information must be considered and implemented by companies as each of their products (the EU also imposes “Privacy by Default”). Under a privacy-by-design regime, any technology like biometric security or verification that relied on capturing and holding information that a person may wish to keep private must be limited or removed in favor of a less intrusive technology that might achieve similar results.

Beginning on May 25, 2018, the EU’s new General Data Protection Regulation (the “GDPR”) will govern the collection, storage, and use of biometric data of individuals in the EU. Adoption and implementation of the GDPR is the most significant change in EU data protection law in more than 20 years. Under the new rules, biometric data is broadly defined as “personal data resulting

---

from specific technical processing relating to the physical, physiological or [behavioral] characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [i.e., fingerprint] data. 5 Unlike some of US state law definitions, the GDPR definition includes both physical and behavioral categories of biometric data. The definition is drafted broadly so it might catch evolving biometric technologies. But EU regulators have yet to interpret how broadly or narrowly these characteristics will be applied, especially what qualifies as a “behavioral characteristic.”

The GDPR categorizes types of data and regulates management of the information depending on the category. Under this scheme, biometric data is classified as a “special category of personal data”; and such data is subject to the strictest rules. 6 For example, regulated entities cannot collect, store or use biometric data unless they have a legal reason. The GDPR then provides a list of the few reasons it would find acceptable, such as (1) explicit consent of the individual, or (2) that use of the data is necessary to carry out obligations related to employment, social security and social protection law or (3) that such use is necessary to protect vital interests of the individual and the individual is not capable of giving consent. Nowhere are legitimate business or security reasons enumerated for holding consumer biometric data. We can assume that many of the business advantages that US companies receive from their use of biometric data will be considered illegal under the GDPR when it comes into effect on May 25, 2018.

The GDPR exemplifies an attempt to regulate these data under a holistic, rather than piecemeal, approach. However, the GDPR sets the floor for regulating biometric data collection and use, and EU Member States are authorized under the GDPR to impose additional restrictions. We must wait and see how Member States may choose to further limit the processing of biometric data.

B. US States Protecting Consumers from Business

Unlike Canada and most European countries, the US federal government has not passed privacy or data laws that either specifically address biometric readings or that could be construed to prohibit private people and entities from taking biometric readings of US citizens. But laws in a few US states directly restrict what biometric readings businesses can capture and store from residents of those states, and state legislatures have provided a cause of action for either individuals or the state attorney general’s office to sue companies that violate these laws. None of these laws completely proscribes biometric capture, but instead they require consumers to be given options to avoid providing physical measurements to the businesses.

Three states (Illinois, Texas and Washington) currently have laws that specifically address collection and use of biometric information by natural persons and private entities. The laws of these three states require persons or businesses provide notice and consent about the collection and use of biometric information and prohibit the selling of such information.

Most recently, Washington passed House Bill 1493 in May 2017. 7 Washington’s statute regulates biometric primary as it relates to commercial activity. Specifically, Washington regulates the “enrollment” of biometric identifiers for

The US federal government has not passed privacy or data laws that specifically address biometric readings. Some states have, but these vary greatly state-to-state.

a commercial purpose. To “enroll” biometric information, a business must do three things: (1) collect biometric identifiers, (2) convert them into a reference template that cannot be reconstructed into the original collected image, and (3) store and use them in a database that matches the information to a specific person. If a business enrolls biometric information, the business must provide notice, obtain consent or provide a mechanism to prevent further use of biometric identifiers for commercial purposes, unless an exception applies.8

Washington’s law allows businesses to collect biometric information for other purposes. For example, businesses otherwise subject to the rules do not have to provide notice and consent to consumers to collect, capture, enroll or store biometric information for a security purpose. Washington’s law also contains exemptions for covered entities or business associates subject to Health Information Portability and Accountability Act (HIPAA), financial institutions subject to Gramm-Leach-Bliley Act (GLBA) and law enforcement officers.

Businesses are more restricted under the Illinois and Texas laws.9 Illinois’s Biometric Information Privacy Act (BIPA) is triggered when a business collects, captures, purchases or otherwise obtains of biometric information, and Texas’s law is triggered when a business “captures” biometric information. Washington’s statute is narrower than both the Illinois and the Texas statute. Unlike Illinois and Texas, Washington’s law is triggered when businesses “enroll” information. Because “enrollment” requires all three activities, Washington does not prohibit, for example, only the collection of biometric information.

States also differ in their definitions of biometric information. Washington defines a “biometric identifier” to include data generated by automated measurements of an individual’s biological characteristics. It gives examples such as fingerprint, voiceprint, eye retinas and irises. But it excludes “a physical or digital photograph, video or audio recording or data generated therefrom.” It also excludes information collected for purposes under HIPAA. Texas defines biometric identifier as a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry, but includes no exceptions for photographs or data generated from them. Illinois has the same list as Texas, but also excludes information like writing samples and photographs. The Illinois definition is still in flux as court interpretations of the law proliferate.

Court interpretations of Illinois’ biometric restrictions are beginning to make waves, but similar decisions have not yet arisen under the Washington law or the Texas law, maybe because exclusions to the biometric identifier definition do not encourage facial scan lawsuits against defendants like Facebook, Snapchat and Shutterfly.10 Probably more significant is the practical impediment that Washington and Texas only allow attorney general lawsuits to pursue violations of these biometric restriction laws, and individuals do not have standing to successfully file private rights of action. State attorneys general operating with public funds are rarely as aggressive in enforcement as the private plaintiff’s bar.

The breadth of the Illinois BIPA’s definitions also leave much for the courts to interpret. In general, plaintiffs have filed two categories of lawsuits under BIPA. These lawsuits involve either (1) online or social media platforms or (2) employers.

The first category of cases, users of online platforms allege that the platforms are collecting biometric information in violation of BIPA, but the platforms argue that their activity is outside the scope of BIPA. These cases are interpreting the bounds of the definition of biometric identifiers and biometric information under BIPA. In these cases, plaintiffs argue that BIPA regulates information at issue because, for example, a map of facial geometry that was generated from photos posted to Facebook qualifies under the biometric identifier or biometric information definitions, and therefore the defendant would be required to offer Illinois residents an option to forgo the biometric data collection. In February and March 2018, two decisions allowed plaintiffs to proceed in their cases, finding that non-compliance with BIPA’s notice and consent requirements were sufficient injury.\(^1\) Some cases have settled, but others are still ongoing at the time of this writing.

Employers using biometric information may also be at risk of litigation for biometric privacy violations. For example, an employee sued supermarket chain, Roundy’s, for a violation of BIPA when Roundy’s failed to provide the required notice and consent to its employees before collecting and retaining fingerprint information it used for timekeeping.\(^2\) This case is another example of the broader reach of BIPA. Unlike Washington, which allows businesses to collect biometric information from employees for security purposes without providing notice and obtaining consent, Illinois requires employers to collect from employees a written release prior to collecting any employee biometric information and as a condition of their employment.

Because direct legislation of biometric privacy has been a creature of state law in the US, businesses often have to default to the most restrictive laws or avoid activities in those restrictive states. For example, Google Art and Culture recent popular search and comparison app which purports to use an uploaded selfie to match a person’s face with faces in famous artworks throughout the centuries, was not offered to residents of the states of Illinois and Texas, with Google apparently fearing a slew of lawsuits in Illinois and broad interpretations of both states’ biometric restriction laws.\(^3\) As companies and legislatures react to this new set of consumer privacy rules, perhaps Washington’s well-considered approach will be adopted by other states seeking to protect their residents’ biometric privacy. In the absence of uniform law or federal requirements, businesses must constantly monitor the statutory and regulatory landscape as state legislatures grapple with the biometric privacy question.

---


\(^3\) Hamza Shaban, A Google app that matches your face to artwork is wildly popular. It’s also raising privacy concerns., The Washington Post (Jan. 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/01/16/google-app-that-matches-your-face-to-artwork-is-wildly-popular-its-also-raising-privacy-concerns/?utm_term=.1484f72cffe0
C. States Protecting Citizens from Government Overreach

Many state legislatures seem concerned about their state bureaucracies capturing and holding the biometric data of their citizens. While no current US state laws limit the use of biometrics by law enforcement, several states have restricted other organs of the state from keeping databases of physical features of state residents.

States in the US are not consistent in their approach to the collection of biometrics for issuing photo IDs differently. For example, Vermont prohibits its Department of Motor Vehicles from using biometric technology in connection with issuing photo IDs. On July 18, 2017, Vermont’s Attorney General concluded that the state’s DMV was violating Vermont law by using facial recognition technology to scan a database to detect identify fraud. The Vermont DMV has suspended its use of facial recognition technology. Similarly, other states like Maine, Missouri and New Hampshire prohibit state agencies, such as the DMV, from collecting biometric information in connection with ID cards or licenses. In contrast, most states are like New York which does not prohibit its state DMV from collecting biometric information as part of issuing its drivers licenses.

Many states are particularly protective of children, prohibiting schools and other public entities from collecting the biometric data of minors in their states. Schools across the US have used fingerprint, iris or vein recognition scanners to replace student ID cards, take attendance, or notify parents where their children get off the school bus. As of 2014, about seventy percent of West Virginia public school districts are using IdentIMetrics Biometric ID Management® biometric technology for attendance and to track students. This activity has disturbed some state legislatures, starting with Florida, which broadly banned the use of biometric identification in schools. Other states, like Louisiana, require advance notice and parental consent before any biometric information can be collected by schools. States are actively introducing bills and passing laws to protect K-12 students, but do so in a variety of ways.

Some states prohibit schools from collecting biometric information (some with an exception for state or federal requirements) and others prevent the release of biometric information without a parent or child’s consent.
D. **US Federal Regulatory Actions**

While the US Congress has not addressed biometrics directly, nor has it passed a broad cross-sector personal privacy law in thirty years, US federal regulatory bodies have taken upon themselves the authority to prohibit certain collection and storage procedures for consumer biometric readings. Section 5 of the FTC Act allows the Federal Trade Commission (FTC) to penalize companies for unfair and deceptive acts and practices, which the Commission, with the support of courts, has interpreted broadly to allow deep investigations of consumer privacy and security issues. The business use of biometrics has fallen within this purview recently.

The FTC is the de facto federal agency regulating privacy and data security across industries on behalf of consumers. To date, the FTC has only spoken to facial recognition. The FTC has published a non-binding guidance document, “Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies,” to highlight its recommendations to companies using or seeking to use facial recognition technologies in their businesses.\(^2\)\(^2\) Even though the guidance is non-binding, the FTC hints that a company’s failure to notify its customers of the company’s practices may result in an FTC investigation or enforcement action.

In addition to best practices for facial recognition, the FTC has approved the use of a facial recognition procedure as a form of verifiable consent under the Children’s Online Privacy Protection Act (COPPA).\(^2\)\(^3\) Parents provide two pictures, the first is a photo of a form of photo identification, like a driver’s license or passport, and the second is a “selfie” (it must be “live” photo and not a still). The second photo is compared to the photo in the ID using facial recognition technology. This process must include privacy safeguards, like encryption and limited data retention (must delete within five minutes of collection). Further, the business must not use the information for any other purpose.

Even though the FTC has provided little formal guidance on the collection and use of biometric information, companies should avoid any practices of collecting and using biometric information that may qualify as “unfair or deceptive.” Businesses found to engage in unfair and deceptive trade practices may be subject to heavy fines imposed by the FTC. Biometric identifiers, including finger and voice prints, are one of 18 HIPAA identifiers that, when combined with a person’s physical or mental health or condition, health care, or payment for health care, are regulated “protected health information.”\(^2\)\(^4\)

Whether granting individuals a human right to control biometric information about themselves, requiring notice and consent to capture biometric data, or simply proscribing methods and means of collecting biometric data, governments have begun to limit the use of this technology for identification and security purposes. Over the next few years, more jurisdictions will consider adding these limitations, and the biometric laws on the books will continue to be interpreted by courts and regulators. The current status of law in this space will continue to change.

---


\(^4\) See 45 C.F.R. § 164.514(b)(2).
Potential Biometric Government Limits That Do Not Yet Exist

Government limitation of biometric capture, storage and identification has only begun recently, and despite the varying directions of current legislation and regulation, many other possible restrictions are likely to be considered and enacted in coming years. The approach of the EU and Canada is relatively broad, basing its biometric limitations on the human rights of each individual, so that any use of biometrics can be analyzed in the light of the subject’s rights and consent. The more piecemeal approach of the US and many other developed countries leaves logical gaps in treatment of the technology. Those gaps may always remain, or may be filled by one or more of the following strategies.

A. Protecting Citizens from Law Enforcement

The most extensive databases of American citizens’ biometric measurements are held by the US Department of Homeland Security and its affiliated agencies pursuant to 28 USC. § 534. Since 1924, the FBI has collected and stored fingerprint records to identify suspects and to share with other law enforcement agencies. The Fingerprint Identification Record System (FIRS) includes much more than criminal suspect or convict fingerprints. It also includes the fingerprints of federal applicants and employees, United States military, aliens, and others including military detainees and other people of interest to the NSA. This system was automated in 1999 so that it can store and compare fingerprint data in digital formats.

Over 190 law enforcement labs contribute to and use NDIS for a variety of reasons. DNA database items are shared with states on a wide area network that can be accessed by state and federal law enforcement agencies. The FBI can remove a state law enforcement agency’s access to NDIS if the required privacy procedures are not met.

The Combined DNA Index System (CODIS), also operated by the FBI, captures, stores and compares personal DNA samples on behalf of law enforcement. CODIS contains discrete databases for missing persons, convicted offenders, and forensic samples collected from crime scenes. The National DNA Index System (NDIS) of CODIS allows disclosure of DNA samples and records from the national database only

1. to criminal justice agencies for law enforcement identification purposes;
2. in judicial proceedings, if otherwise admissible pursuant to applicable statutes or rules;
3. for criminal defense purposes, to a defendant, who shall have access to samples and analyses performed in connection with the case in which such defendant is charged; or
4. if personally identifiable information is removed, for a population statistics database, for identification research and protocol development purposes, or for quality control purposes.25

Over 190 law enforcement labs contribute to and use NDIS for a variety of reasons. DNA database items are shared with states on a wide area network that can be accessed by state and federal law enforcement agencies. The FBI can remove a state law enforcement agency’s access to NDIS if the required privacy procedures are not met.

25 34 USC. § 12592(3). The FBI has authority to establish and maintain the NDIA under the DNA Identification Act of 1994.
Security professionals at airports in the US and around the world are collecting face geometry readings and making comparisons to known terrorists. Massachusetts senator Ed Markey noted that, given the current efficiency of the airport system, four percent of Americans are or will be improperly flagged by scanning programs.26 The US State Department holds an enormous database of human facial measurements. As of December 2009, its Consular Consolidated Database contained more than 75 million photographs and is growing at a rate of approximately 35,000 records per day.27 According to a Georgetown University study released in 2016, half of Americans faces are captured in law enforcement databases — about 117 million adults. The study states “[w]e are not aware of any agency that requires warrants for searches or limits them to serious crimes.”28

According to the Government Accountability Office, as of the summer of 2016, sixteen states allow the FBI to use facial recognition to compare faces of suspected criminals to the state’s driver’s licenses or ID photos, creating an enormous line-up of primarily innocent people examined in criminal investigations by algorithms rather than humans. According to the Georgetown study, researchers obtained documents stating that at least five “major police departments—including agencies in Chicago, Dallas and Los Angeles—either claimed to run real-time face recognition off of street cameras, bought technology that can do so, or expressed an interest in buying it.”29 So people off the street are being matched immediately with pictures in this database. The Maricopa County, Arizona sheriff’s office under Joe Arapaio downloaded every driver’s license and mugshot from every resident of Honduras into its facial recognition database.

If legislatures are concerned about biometric capture and storage without consent, about the vulnerability of biometric databases, and about government overreach, why have these extensive and, in many cases unwarranted, collections never been questioned? How can the U.S federal government collect DNA samples on millions of its own citizens, holding the core code to each life encapsulated within its DNA, and not have legislators attempt to limit access to the code and its many and varied uses? Why can the police in the United States put more than half of their people in machine-read criminal line-ups every day and not have this practice questions by the people’s representatives?

Some legislators are taking aim at law enforcement’s broad authority to use biometric data. For example, in 2018, California Assembly Member Lorena Gonzalez Fletcher introduced a bill requiring police to obtain a court order, search warrant or written consent from the subject and subject’s parents before

---

collecting DNA from a minor. In March 2017 the Maryland House of Delegates passed a bill to form a taskforce to study police use of facial recognition software and other surveillance technologies.

Given this backdrop, on September 21, 2016, the ACLU launched the Community Control Over Police Surveillance (CCOPS) effort to pass laws that ensure residents, through local city councils are empowered to decide how surveillance technologies are used. In 2017, Seattle; Nashville; Somerville, Massachusetts; and Santa Clara County, California passed CCOPS laws restricting certain surveillance techniques, and such laws have been introduced into more than a dozen other cities, plus the legislature of California and Maine. This movement may become more specific and address some or all of the biometric surveillance instituted by police departments nationwide, as well as the explosion of license plate reading technology (biometrics for cars) in city and state police forces. Placing limits on police use of biometrics is not a significant movement yet in the US, but with the mass of information currently collected under little or no legal or public supervision, the area is ripe for legislative attention.

In the US, law enforcement use of biometrics to identify, arrest and convict suspects has Constitutional implications and further limitation on the police biometric programs may arise from Constitutional challenges in court. Some cases have cited the Fifth Amendment protection against self-incrimination to protect an individual’s right to refuse offering fingerprints or DNA when requested by police. Under current US law, the Fifth Amendment protects a citizen from being forced to divulge an account or device password to the police, but does not protect refusal to provide a fingerprint or faceprint to open an iPhone. This distinction could be changed by legislation or contrary court rulings, but as of now, a fingerprint or faceprint is considered a physical attribute and therefore not protected by the Fifth Amendment, while a remembered password would require a verbal or written “testimony” against the holder. In February 2017, a Federal magistrate judge in Chicago found that a forced fingerprint password reveal might be testimony against oneself protected by the Fifth Amendment, but this opinion is in the clear minority.

Most of the Constitutional cases in this space involve the Fourth Amendment protections against unlawful search and seizure. Even the Federal case in Chicago discussed immediately above was ultimately decided on Fourth Amendment grounds, with the court finding that a warrant was needed to compel a suspect’s thumbprint to open the suspect’s smartphone. Fourth Amendment provides “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” And nothing can be more directly relevant to an individual’s security in her person than actual measurement of personal physical characteristics.

As technology changes, growing the amount of information about us that can be collected and stored, and constantly improving the computerized

A few US cities, including Seattle, Nashville, and Santa Clara county, are restricting certain biometric surveillance methods by law enforcement.

---

33 US Const. amend. IV.
methods of categorizing and analyzing this information, US federal courts seem to be the final possible check on law enforcement’s abilities to know everything about us all the time. For example, in 2012, the US Supreme Court held in a unanimous decision that the Fourth Amendment prohibited 30-day constant mechanized surveillance (via GPS) of a person’s automobile without a warrant. In 2014, the same court changed much of the widely held law-enforcement-centric interpretations of the Constitution and held that police need a warrant to search digital information contained in an arrested person’s cell phone.

However, when it comes to biometric protections, the US Supreme Court has not been as quick to raise the shield of the Fourth Amendment to protect individual rights as lower courts. For example, in 2013, in a 5-4 decision, the Court ruled that it is not a violation of the Fourth Amendment for the police to take a DNA swab from the cheek of a person under valid arrest without a warrant. As discussed above, DNA provides vast amounts of information about a person—much more than face or fingerprint pictures—from his health to his proclivities, and can obviously be used to compare to crime scene evidence. Prior to 2013, federal law enforcement and 28 states allowed police to make unwarranted DNA capture and searches of arrestees, and the Supreme Court opened the practice to the rest of the jurisdictions, and the person’s DNA can be used to search for other possible crimes even if the police were wrong to make the arrest.

Where else will warrantless DNA checks be allowed under the Fourth Amendment—traffic stops, border checks, or random stop and frisk actions? Collection is not the not the only search and seizure concern with DNA capture. Once a person’s DNA is taken by police and placed in the system, what can be done with it? We clearly allow new samples to be compared against criminal evidence databases, running deep checks for criminality for anyone arrested for any reason. DNA can be used to predict alcoholism and arguably even a predilection for violent behavior. Could arrestees or subjects of traffic stops be checked for the “violence gene” and held longer in jail because of their genetic structures? Would harsher treatment for people with suspect genes violate the Fourth Amendment protections against unlawful search and seizure? It is likely that only the courts would place limits on law enforcement uses of DNA readings, as no US legislature or regulator has seemed inclined to do so. Watch for courts to distill the limits of what police can do to take and use our biometric readings, including DNA.

### B. Restricting certain Biometric Technologies

Thus far, no US legislature, regulator or court has seen fit to place legal restrictions on capture, storage or analysis of any specific type of biometric reading.

37 Study 2014 from Karolinska Institutet, Sweden “analyzed the genomes of 895 people who were found guilty of a total of 1,154 crimes, including murder, manslaughter, and attempted homicide and battery. Each one of these criminals had genetic variants of either the MAOA (monoamine oxidase A) gene or the CDH13 (cadherin 13) gene, with the strongest associations found among those whose crimes were considered ‘extremely violent behavior.’ Overall, they found that people with these variants were 13 times more likely to have a history of repeated violence. Meanwhile, those in a control population of Finnish residents with no history of violence showed no signs of the variants. Overall, the researchers estimated that five to 10 percent of violent crimes in Finland could be attributed to people with these genes.” Quoted in article by Anthony Rivas in Medical Daily, Oct. 29, 2014.
to analyzed facial recognition technology, there has yet to be a legal restriction of its use. Similarly, while DNA capture and analysis can lead to deeper facts about an individual than the person herself is likely to know, no one has passed a law that restricts DNA reading by anyone – law enforcement, medical science, corporations or the general public. If you wanted to start your own DNA database and you had the money and the expertise to do so, US law would allow it. If you wanted to take swabs of where people’s fingers had touched hand balance straps on the public buses, you could legally do so.

The Utah legislature passed an unusual measure allowing children conceived via sperm donation access to the medical histories of their biological fathers, thus expanding the spread of biometric information by law.38 Otherwise, despite voluntary guidelines, the reproductive assistance industry in the United States has very little direct regulation and none on what information about donors or children may be captured, analyzed or placed in databases. Fertility clinics take eggs and sperm from individuals and can test their DNA and other health measurements, applying the test results to files of the subject donors.

No one in the United States government seems interested in restricting the spread of any named biometric technology that may seem more dangerous or intrusive than any others. Specific restriction on capture and types of use for DNA, retinal scans, fingerprints or even faces is a natural direction for legislation and regulation to take on either the federal or state level. Although it is likely that any such restriction will arise when a particularly disturbing application is publicized or a famous cases arises of abusing biometric captures for nefarious purposes. For example, if news reports were correct and a British tabloid had attempted a honey trap to capture some of Prince Harry's DNA to trace his questioned paternity, legislators might react angrily to the imposition on the Prince's privacy. But until such an outrage is publicized, we are unlikely to see specific biometric technologies restricted.

C. Restricting Classes of people subject to Biometric Review

Some of the US state biometric laws are more protective of children or school students than other people. However, aside from this minor and understandable limitation, there are no limitations on biometric capture that protect specific classes of people. Laws differentiate between classes of people in many cases. For example, US laws against discrimination tend to divide the population down into protected categories that have traditionally suffered discrimination, who are protected by these statutes, and the rest of the population, which is not so protected. These classes may be divided by race, religion, gender, sexual preference and age, but protected categories receive the benefits of these laws. Some laws distinguish people by occupation and provide additional protections and/or responsibilities by the role a person plays in society. Licensed doctors, attorneys and accountants have higher standards placed on them and some benefits attached to the status. Military service includes a set of benefits and protections. Felony conviction includes restrictions not only on freedom but on a convict’s rights as a citizen.

Legislators have not yet divided out classes of people, other than some limited protections for children, that are subject to biometric tests or protected from biometric capture. We could argue that the court-created doctrines of Fourth Amendment protections and limitations on those protection for persons arrested or convicted are personal-status based biometric distinctions, but these are not legislative enactments. It is possible that more future statutes will distinguish what type of people — citizen vs. alien, minor vs. adult, privileged vs.

---

non-privileged, arrested vs. free – are subject to biometric search and capture, and which databases can be built with the biometric information from a legally distinct group.

**D. Time Limitation on Storage**
The GDPR includes a provision that personal data, including biometric data, may only be kept by a business for the minimum amount of time needed to perform the legally-allowed task with that information, subject to very limited exceptions. After that time, the data must be erased from company databases unless there is another specific legal reason to keep it. Further, the biometric privacy laws in Illinois, Texas and Washington also require information to be deleted after a certain time.

In Illinois, companies must develop a written policy with a retention schedule and make it available to the public. The retention schedule must include the company’s guidelines for permanently deleting biometric identifiers and biometric information the company has collected. The law requires such information to be deleted by the earlier of (a) when the initial purpose for collecting the biometric information has been satisfied or (b) three years of the individual’s last interaction with the company. In Texas, companies must destroy biometric information “within a reasonable time” but not later than one year after the purpose for collecting the information expires (unless an exception applies). In Washington, companies may retain biometric information for no longer than it is reasonably necessary to: (a) comply with a court order or law; (b) protect against or prevent actual or potential criminal activity, security threats, or liability; and (c) provide services for which the biometric information was enrolled.

**E. Rule that Biometrics be converted to Non-Reversible Reference Templates**
One of the most sensible requirements that any governmental entity could possibly make in relation to the use of biometric measurements is to rule that the biometric sample captured from any individual be stored not as a directly readable picture, but instead by stored as non-reversible reference templates created by encryption technology. Databases of biometric samples converted by algorithms and stored as templates could not be used to identify the biometric subject by anyone who stole the information from that database. The thief would not be holding a usable fingerprint, faceprint, voiceprint or DNA sample, but instead could steal only a useless set of numbers.

Legislation and regulation now unnecessarily restricts collection and storage of biometric data, apparently to minimize the possibility that the biometric database is not secure and the personal information could leak out to malfeasors. However, requiring reference template storage would eliminate the possibility of this harm and allow for less restrictive rules on other aspects of biometric storage. Plus, reference template storage is an industry best practice now, so that requiring storage in this manner would not be a significant technical limitation on the use of biometric technology. While legislatures have not passed significant laws with this requirement, smart lawmakers should think about regulating this space in the future.

Lawmakers should think about regulating the way that biometric data is stored in order to ensure better and less restrictive security.

---

Advising Business How to Operate Under Current Biometric Rules

Certain best practices make sense for companies operating under the current set of biometric statutes in today’s regulatory climate. While biometric capture and analysis rules are not as tight in the US as they are in Canada and the EU, companies can take a few practical steps to keep themselves on the right side of any relevant law in this space. The following policies, procedures and actions will help keep a company from trouble with biometric identification of consumers and/or employees.

A. Consent of the Subject

One rule seems to be consistent in compliant biometric systems; they favor requesting and receiving consent of the biometric subject. In the law of privacy, consent is king. Legal regimes like the EU that place restrictions on the capture, storage and use of personal data, generally allow use of the personal data if the data subject consents to the behavior. So if your company wants to minimize compliance issues when collecting and applying biometric information, then it should request consent to collect the data and additional consent for the intended use of the data.

The more specific the consent, the better it will be treated under law. So if your company grabs voiceprints of everyone who calls into its consumer hotline, and each of those people is simply asked if their voice may be used later by the company, then your company has not received the kind of consent that is necessary to overcome legal proscriptions. Instead you must ask if that voiceprint may be used as an identifier for comparison for future calls, or if it might be placed into a database and activated when the company wants to verify an account holder’s request live at retail branches. The data subject must understand what she is consenting to in order for the consent to be compliant with many laws.

In addition, in the EU and elsewhere, a data subject always has the right to withdraw her consent to use biometric information.43

B. Tailor Technology to Task

Biometric data can be valuable for many different reasons, and it is the perfect authentication or authorization device in many cases. However, taking biometric readings from your customers or workers may also be unnecessary to do some jobs. For example, using biometric authentication for 50 cent purchases from a candy vending machine is an unnecessarily protective technology for the task. Biometrics may not needed for the security job that you are contemplating, and if that is the case, then apply a less intrusive technology. The new EU rules require that the least intrusive technology be used for each task, and biometric capture and comparison is a very intrusive

It is much less intrusive to ask a question or to require a person to carry a magnetic passcard than it would be to take a biometric reading from that person (e.g., capturing fingerprint or facial geometry). Under this logic, nearly every method of identification is less intrusive than capturing, storing and accessing a person’s DNA profile, with is arguably the most intimate and intrusive measure of all. Making DNA comparisons can allow for highly specific identity matches where identity is crucial and huge dollars or vital security are on the line. But DNA is too intrusive and provides much more information than most security systems need, so that a fingerprint or facial scan may be a more appropriate measurement. Make sure it is needed where it is used.

C. **Reduce Storage Time**

Many privacy rules restrict the time that information is stored—the longer that a company holds onto information, the more likely that the information will be stolen or used for a malicious purpose. In addition, why waste storage space holding onto personal data that is no longer needed? A business should reduce the time it holds onto data to the minimum time necessary to effectuate the business purpose for the data.

D. **Convert Biometric Data to Reference Templates**

As discussed above, biometric data should never be stored in a fashion that would allow theft and use of the biometric sample. Instead, it should be mathematically converted to reference file so that only the program that captured the biometric reading can make comparisons to it, and so that no one who steals the file can use it in any manner. In 2018 or later, there is no excuse for managing a biometric identity system in any other way.

E. **Creepiness Factor**

How intrusive is the biometric technology that your company wants to use, and how aware are your customers or employees that their measurements are being taken? Under what circumstances is the data taken and what is the function of making these physical comparisons? What parts of a person’s body needs to be exposed to measure your biometric identifier and can a person present herself for measurement without exposing himself to the germs or body of another person? While the general public is currently accustomed to signing checks and even to using fingerprint scanners, other biometric capture techniques are likely to lead to resistance from people who find them strange and uncomfortable. Even if your biometric system is too efficient, for example, identifying a person from a face picture taken 40 years ago, it may make people uncomfortable.

For this reason, being on the cutting edge of biometric identification systems is not always the best policy. People may refuse to use technology that they find to be too intrusive or likely to lead to catching the flu from the previous person who used the capture machine. Some measurements are embarrassing or just plain creepy, and employees may resist a requirement to submit themselves for measurements. So consider the understandable sensibilities of the people your company is measuring and only insist that they participate in a biometric system that they are likely to find comforting.

---

Conclusion

A decade ago all talk of the law of biometrics was speculative. Now certain rules, laws and restrictions exist and more are being considered all the time. Without an understanding of the way biometric systems work, and what tasks they do best, companies and legislators will misunderstand the technology and risk deploying it improperly or legislating against it needlessly. By seeing the fundamental nature of biometric measurements we all can apply the technology for its best effect, and make our world safer for it.