

Risks and Opportunities of Contactless Biometrics

2017 Public Private Analytic Exchange Program
September 2017

Research Team

Last Name	Organization
Matthew Brainovich	DHS FEMA
Thomas Decaro	FBI
Jack Furbee	FBI
Ryan Koder	DHS NPPD OBIM
Raymond Lipps	Celgene
Lynn McCloskey	Illinois State Police – Statewide Terrorism & Intelligence Center
Bridget Michaelson	DHS TSA
Brian Ulicny	Thomson Reuters
Matthew Hendley	FBI – Co-Champion
Joey Hixenbaugh	FBI - Champion



Executive Summary

Abstract: In recent years, we have seen great progress in contactless biometrics for entities requiring accurate and expeditious identification. In this whitepaper, we address the state of the art technology and techniques in identifying individuals using contactless biometrics such as face, gait and voice recognition for the purposes of identification, investigation and authentication of individuals. We examine the limitations and challenges and identify the obstacles that must be overcome in order for this technology to reach its full promise. In particular, we examine ways in which law enforcement agencies and private sector companies can leverage these new forms of Personal Identifying Information (PII) without encroaching on civil liberties or compromising intellectual property. We conclude with recommendations for the path forward in public/private collaboration in this area.

Methodology

Key Questions:

- What is the current state of biometric technologies? How is it collected, and how are agencies and/or the private sector using them?
- What are the limitations and challenges of collection biometric information (i.e. privacy concerns, budget, accuracy, standards)?
- What is the ideal future state of biometric information collection and how do we overcome the limitations to get there? How do we ensure the accuracy of biometric information collection systems? How do we mitigate privacy concerns?

Section 1: Current State of Biometrics

Digital identity identifies a person based on (one or more of):

1. What they know (e.g. a password or challenge question)
2. What they have (e.g. a keycard, CAC card)
3. Who they are (biometrics)

Biometric systems involve *enrollment*, in which a *template* or various specific bodily measurements are taken, and a *verification* or *identification* process in which a new set of measures is matched against either the entire set of identifiers (identification) or a particular subset of templates (verification) to either identify a specific person or verify that the person at hand matches presented biometric credentials.

Providing access to systems or privileges on the basis of biometric identifiers requires extra security because a person's biometric identifiers can't be replaced. Therefore, if a person's biometrics identifiers are compromised in ways that enable a third party to spoof their identity, there is little remedy within the system that can be provided. A person cannot be provided with new facial geometry or fingerprints in the event that these are compromised in the same way that they can receive a new password or access card.

Nevertheless, if handled properly, contactless forms of biometric identifiers can be used effectively and are increasingly being adopted. Industry experts told us that they see only three forms of contactless biometrics being currently viable: face recognition, iris recognition and (contactless) fingerprint identification. We will focus on these in this report.

Face Recognition

Currently, large-scale deployments of face recognition are taking off around the world, and new technologies are already being tested and implemented by governments and the private sector for a variety of commercial and security purposes. Facial recognition biometric systems are typically composed of four basic components: 1) a camera device to capture an image; 2) an algorithm to create what is called a facial template; 3) a database of previously stored images; 4) and another algorithm from which you can compare a captured image to the database of images or a single image within the database.ⁱ Facial recognition systems are used for a variety of purposes by both the public and private sectors, including marketing, security, and investigation. Throughout this research process, our team interviewed a number of biometric technology experts on the current state of biometric technologies, including face recognition technologies. According to one of the experts we interviewed, "deep learning" approaches to face recognition using "convolutional neural networks" represent the state of the art and achieve performance levels like human beings.ⁱⁱ

Commercial Marketing and Asset Security

On the commercial front, although the full extent to which facial recognition systems are used by the private sector is unknownⁱⁱⁱ, companies have been and are continuing to implement facial recognition technology for a variety of purposes, from marketing to personal user and asset security. Utilizing facial recognition technologies and software, companies are creating new and innovative services in the hopes of attracting customers. Google's Picasa photo editing software, for example, uses face recognition to tag names to matching faces within photographs uploaded into the software.^{iv} Similarly, Facebook uses facial recognition features in its application to aid its users in connecting with their friends and acquaintances on Facebook by automatically identifying persons in photographs with 98 percent accuracy from a vast archive of data that expands every time one of its billions of users uploads a photo and tags someone.^v The electronic commerce giant, Amazon, is also marketing its image recognition software, Amazon Rekognition, for users of its Prime Photos service. Through this software, users are able to detect not only faces, but also objects and scenes in order to make it easier to organize and filter their photos. The facial analysis component of the technology can even, as Amazon asserts, determine the sentiment of the individual in the photograph by analyzing attributes such as mouth shape (i.e. whether or not the individual is smiling or not), as well as create an index of photographed individuals based on their facial attributes.^{vi}

Several major technology companies, including Facebook, Google, and Apple, are also utilizing automatic facial recognition and detection applications in the services they provide and the goods they produce. In this age where more and more communication and transactions are carried out through mobile technologies, the need for securing data and sensitive personal identifying information (PII), is greater now more than ever. Some companies are already looking to facial recognition software for their mobile phones as an added layer of verification, including Apple which is developing a 3-dimensional face scanning feature that will allow users of its future iPhones to use their face instead of the current existing fingerprint recognition login in order to unlock their phones. This technology will also allow the user to access secure apps and authenticate payments.^{vii}

In addition to increased security for the personal user, some private sectors, including retailers, casinos, and banks, are using facial recognition systems to secure their own assets. According to the National Retail Federation, some companies are testing systems that use facial recognition technology with closed-circuit television systems in order to enhance theft prevention measures. Casinos are similarly using facial recognition systems in order to identify suspected gambling cheaters or members of organized criminal networks who seek to defraud them (cite?). Financial institutions have also implemented facial recognition technologies into their security systems to help identify robbery suspects as well, helping to further deter criminal activity.^{viii}

Homeland Security and Identity Verification

Aside from the commercial applications that facial recognition technology has afforded to the private sector, it has also been an integral component in the development and use of biometrics to aid the national security efforts of governments around the world. In North America, as concerns heighten around the potential for individuals to cross borders in order to carry out unlawful acts, Airports throughout Canada and North America have begun looking into the biometric facial comparison technologies for traveler screening programs at exit points.

In Canada, the Canadian Border Services Agency has begun installing kiosks which utilize facial recognition technology at airports throughout the country and will continue rolling out the technology into 2018. The new technology, known as the Primary Inspection Kiosk (PIK) program, will utilize both facial recognition and fingerprint biometrics and hopefully serve to facilitate clearance procedures by decreasing the number of traveler interviews with border agents at primary inspection and allow those agents to focus their attention on passengers who may warrant more rigorous screening.^{ix}

In the United States, DHS's Customs and Border Protection Agency (CBP) tested a similar facial biometrics program at Washington Dulles International Airport, to compare a traveler's face with the image stored on their electronic passport. The goal of the new machines is to improve screening procedures by streamlining the clearance process and reducing the number of traveler interviews with border agents at primary inspection.^x Developed for use by CBP officers at entry points around the county, the technology focuses on over 80 unique facial features, such as distance between the eyes, the depth of eye sockets, the shape of cheekbones, or the length of the jaw line, in order to verify a traveler's identify at entry points.^{xi} "CBP works with stakeholders to build a simplified but secure travel process that not only meets the biometric exit mandate, but also aligns with CBP's and the travel industry's modernization efforts," said John Wagner, CBP's deputy executive assistant commissioner for field operations.^{xii} Following these tests, this technology is now in use at six US airports—Boston, Chicago, Houston, Atlanta, Kennedy Airport in New York City, and Dulles in the Washington, D.C. area—with future deployments planned at more airport exit points in the near future.^{xiii}^{xiv}

CBP is currently leading a trial with JetBlue of facial recognition technology. The system matches images to a government database of Passport Photos. JetBlue announced May 31, 2017 that it was collaborating with CBP on facial-recognition technology from SITA, an airline consortium, to identify travelers at the gate during boarding. The program began this summer with flights from Boston's Logan International airport to Aruba's Queen Beatrix International airport. We interviewed Sean Farrell from SITA, an airline consortium that is piloting this program. In the boarding process, customers who choose to board via face recognition have their photo taken at a custom-designed camera station. This camera connects to Customs and Border Protection to recognize the image to passport, visa or immigration photos in the CBP database associated with

passengers on the flight manifest. See Figure 1. The customer is notified on an integrated screen above the camera when they are cleared to proceed to the jet bridge.^{xv}

This is an interesting scenario in that the face recognition technology is developed and owned by a private airline, and the biometric datapoints are matched against visa, immigration or passport photos held by the US Government.

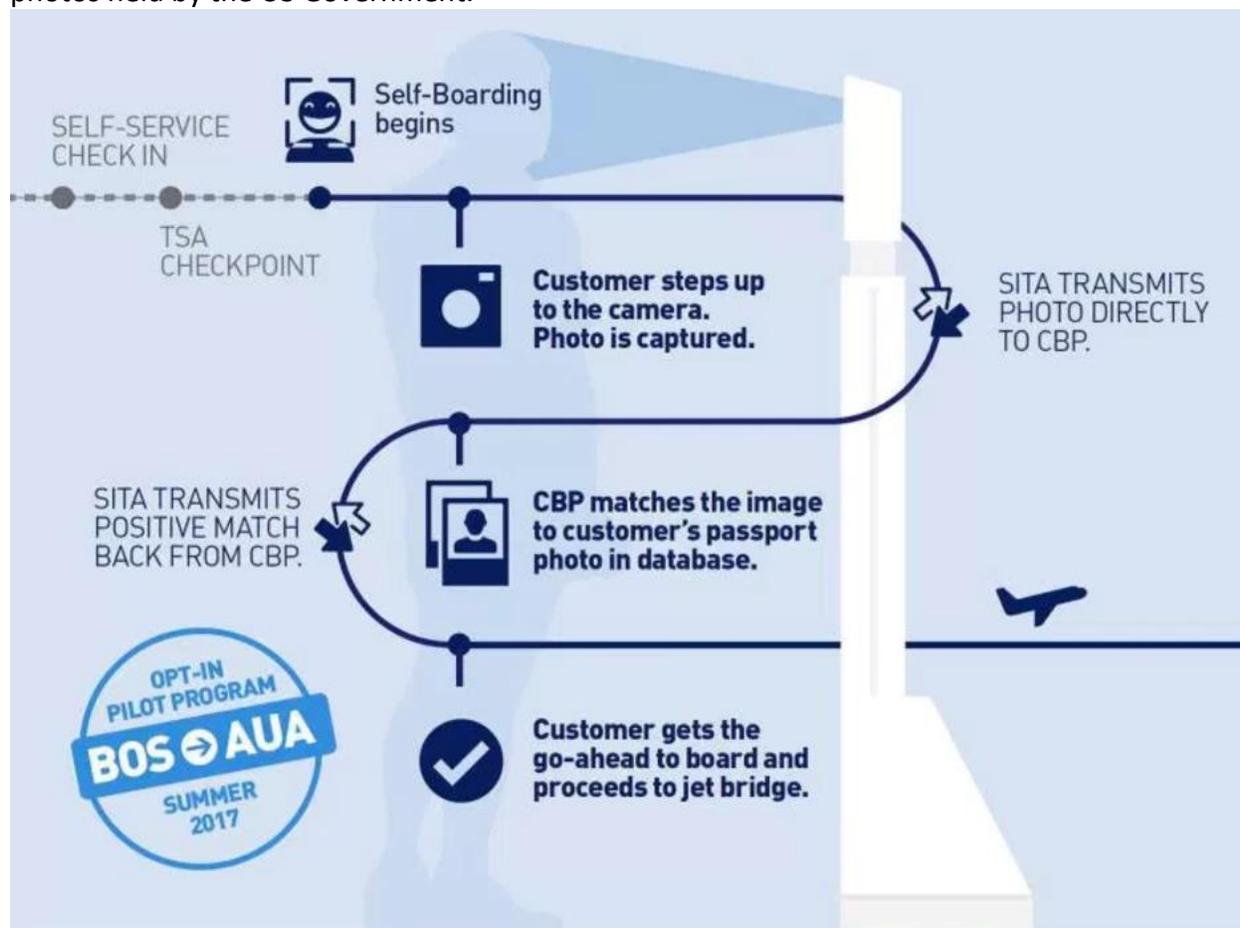


Figure 1 SITA/JetBlue Face Recognition as Boarding Pass system for Boston to Aruba flights, deployed July, 2017. (Image courtesy of SITA.)

According to SITA, each biometric identification takes around 5 to 6 seconds. Adoption of the system is high. The system is somewhat low-risk, because if passenger verification fails, the passenger can simply fall back to the paper or barcode boarding pass. This face recognition system does not involve proof of living (movement) that others do, because the collection is supervised. The exit photos are destroyed after two weeks for US persons; for non-US persons, they are retained indefinitely. Passengers are not required to remove their glasses or hats or other gear, such as neck pillows. Face recognition occurs despite these issues. This system cannot be used for domestic travel, however, since it currently identifies faces against passport and visa photos only, which are not available for domestic flights.

The second system whose representative we interviewed was Voatz (voatz.com), a blockchain- and biometric-based phone voting app that is certified for the 2018 Massachusetts elections (see Figure 2). To register for this system, you download the app on your phone. Then you capture a state-issued ID card, your driver’s license, front and back. The system then verifies that the owner of the phone is the person on the ID card (3). To vote, you sign in to the app, prove that you are living, by taking a "selfie" while initially moving the phone around. Your selfie is then verified against the biometrics stored with your ID card (i.e. the state DMV photo) (2). A fingerprint scan or retinal scan is used to further confirm identity and eligibility to vote. Votes are recorded anonymously and in a tamper proof way on the blockchain (4). The voting results are anonymous and irrefutable.

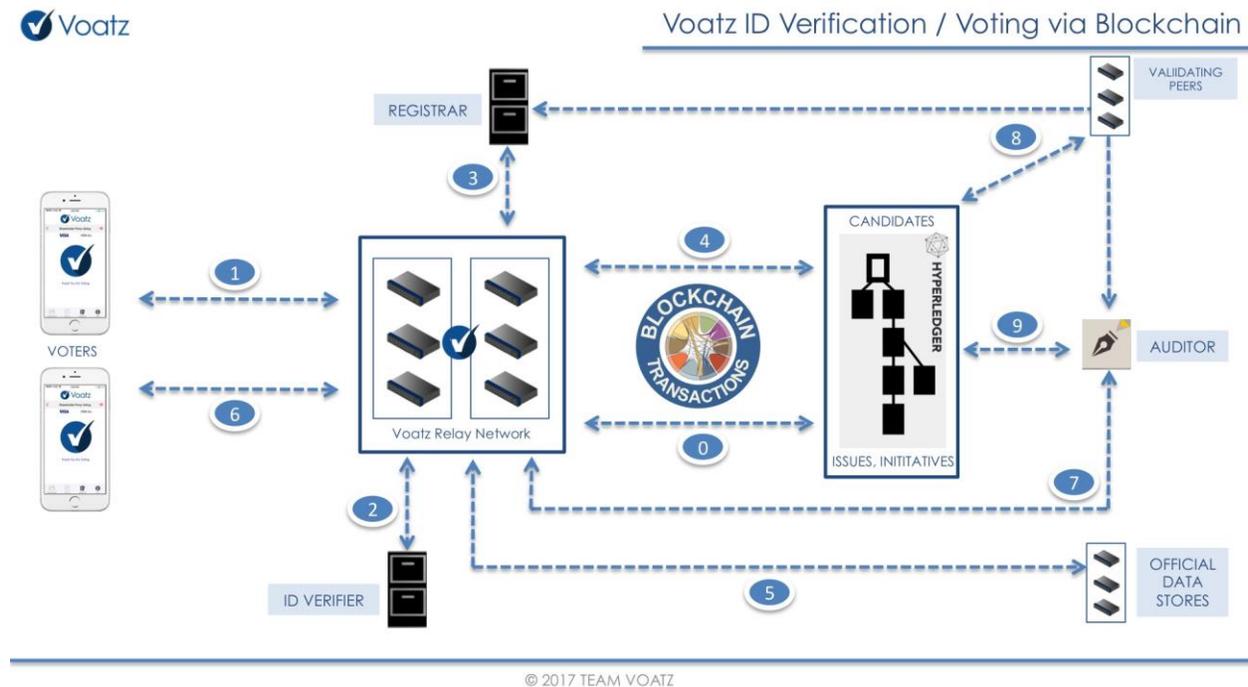


Figure 2 Voatz Flow Diagram (Image courtesy of Voatz.com)

The system was deployed for several low-risk elections (colleges, corporations, political parties), but it will be rolled out for the first state election next year. Not all state IDs conform to sufficiently high standards that they could not be hacked in this system with fakes. Voatz has established which state IDs are appropriate. Voatz believes that this system will enable more people to vote, to avoid the long waits and inconvenience of in-person voting. They note that only one-third of eligible US voters participated in the 2014 elections.

The third private company we interviewed was MorphoTrust, a division of Safran Identity and Security. MorphoTrust and its parent company is perhaps the largest biometrics company in the world. MorphoTrust has provided the biometrics-based authentication for the Indian

government's Aadhaar system, by which 1.1 billion Indian citizens are captured biometrically (contactless fingerprint or iris) and this is used to establish identity for the purpose of government benefits (See Figure 3). Transactions consisting of 15 million a day use Aadhaar, up from 3 million a day in 2016. Four billion authentication transactions have taken place since the program started. Indian Government officials state that the system accurately verifies the identify of a citizen 92percent of the time, and they expect this to rise to 95 percent.^{xvi}

The Aadhaar system had some initial difficulties with older Indian citizens, whose fingers were too dry to provide suitable fingerprints. Iris recognition helps here. Even infants can be iris captured. MorphoTrust provides both the equipment to enroll citizen’s in the Aadhaar program biometrically as well as the equipment to biometrically authenticate citizens. Moreover, because the population to be biometrically identified is so large, the projected false positive rate has been judged to be too high, even under the assumption that citizens are not attempting to have duplicate entries in the system deliberately.^{xvii}

In the Cards

Aiming to improve efficiency and reduce fraud, India will use its new biometric ID system, Aadhaar, to revamp a subsidy program providing cheap food and fuel to hundreds of millions of people. Here’s how buying rice will change.

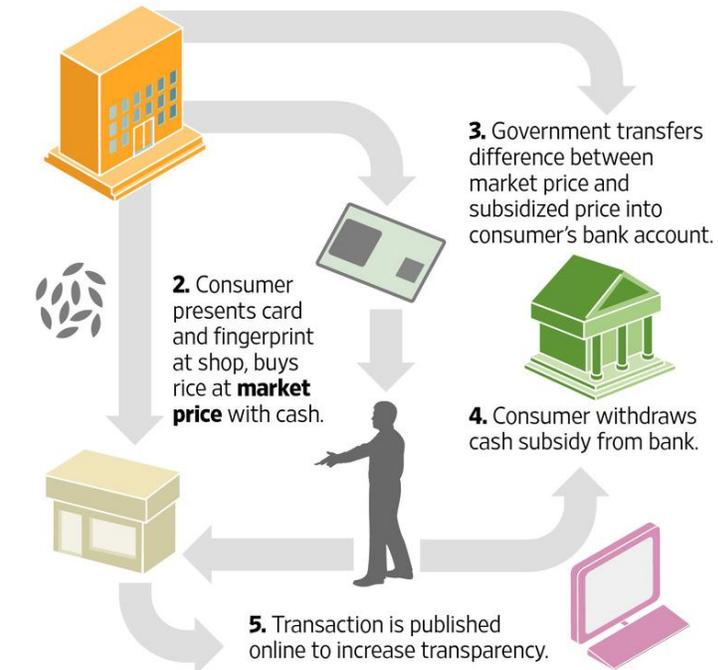
USING RATION CARD

1. Government issues ration cards to consumers, provides rice to participating shops.



USING AADHAAR CARD

1. Government issues Aadhaar card to consumers, provides rice to participating shops.



Source: staff reports

THE WALL STREET JOURNAL.

Figure 3 Aadhaar system flow. Morpho Trust provides the contractless fingerprint registration and identification. (Image: WSJ)

There have been many complaints in regards to the Aadhar system which is currently being adjudicated in the Indian Supreme Court. The system is high-risk, since the provision of benefits depends upon biometrical recognition of the citizen. Even a 0.01 failure rate in India still amounts to a large number of people.

The fourth system whose representative we interviewed was Hypr. Their CEO described their system, in which biometrics are captured in a decentralized way (Figure 4). Every user keeps the biometrics on his or her own phone. In order to sign into a banking web site, for example, the bank website sends a request to the user's phone. The user verifies their fingerprint against a stored fingerprint or other stored biometric, such as a facial biometrics. If it matches, the phone sends a login token to the banking website. This is more secure than a password, which can be hacked or is hard to remember.

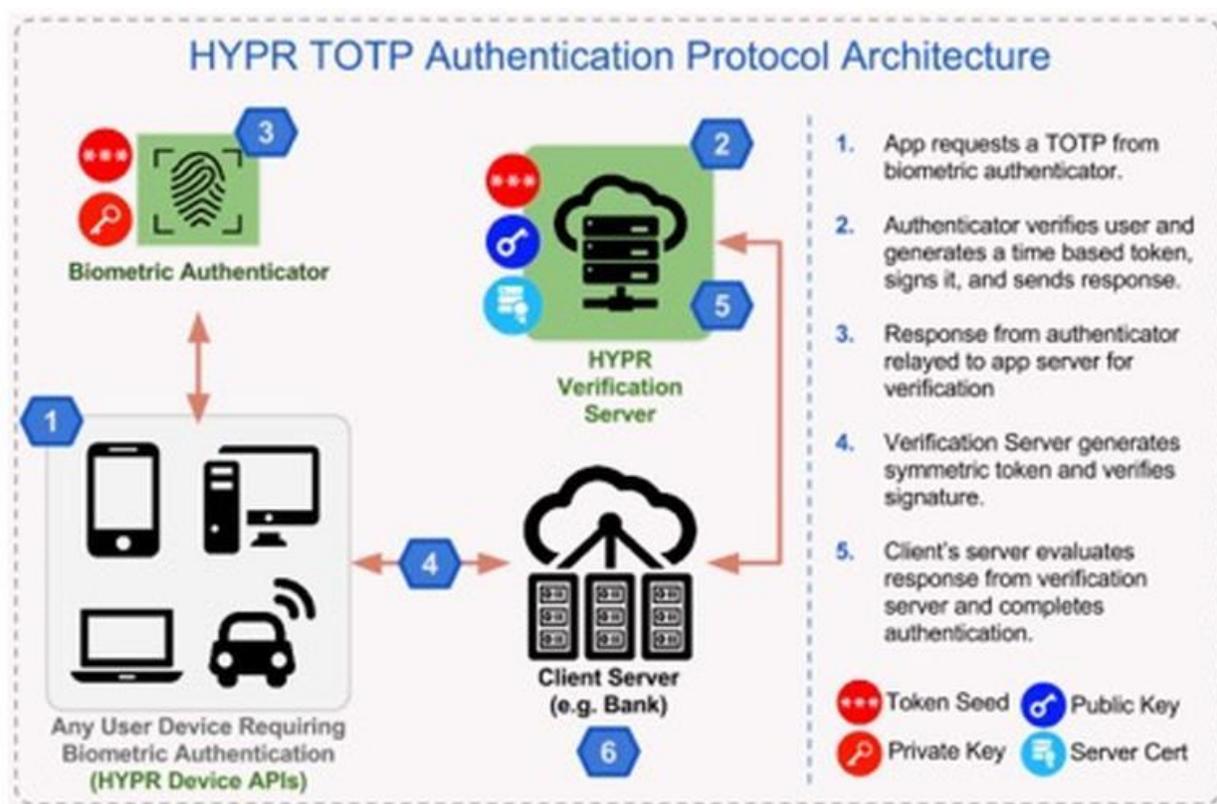


Figure 4 Hypr Biometric Authentication system. (Image courtesy of TechRepublic).

The Hypr platform's server component achieved FIDO certification in April, 2017. The specifications of the FIDO Alliance enable an ecosystem of hardware-, mobile- and biometrics-based authenticators that can be used with many apps and websites. This ecosystem enables enterprises and service providers to deploy strong authentication solutions that reduce reliance on passwords and protect against phishing, man-in-the-middle and replay attacks using stolen passwords.

Law Enforcement

Facial recognition technologies are used heavily by law enforcement entities for investigation and attribution purposes. The Federal Bureau of Investigation (FBI), for example, retains a database of criminal history records complete with a mugshot repository called the Interstate Photo System (IPS) within its Next Generation Identification (NGI) System. The system allows authorized local, state, tribal, and federal law enforcement partners to conduct automated facial recognition searches by submitting a “probe” photo that is compared against a gallery of potential candidate photos of up to 50 individuals, which the law enforcement agency must review manually for further investigation in order to determine if any of the faces are a match.^{xviii} Much of this gallery of potential candidates comes from the databases of driver’s license and ID photos of as many as 30 states.^{xix} Not surprisingly, this heavy use by law enforcement, as well as other Homeland Security entities and even the private sector, has generated significant concerns regarding the limitations, validity, and the potential for undue use.

Contactless Fingerprint

Contactless fingerprinting technologies (CFTs) represent an emergent type of biometric collection which presents enormous potential benefits to public and private users. Although CFTs are somewhat new, their continued development could vastly improve fingerprint collections and analysis over legacy fingerprinting technologies (LFTs). CFTs confer the following potential key advantages over LFTs: faster capture, unattended operations, and ability to capture fingerprints in a hygienic fashion. These advantages are relevant to both the public and private users and uses. However, CFTs are not yet mature, and they face several developmental hurdles. Further, whether they mature and eventually overcome these developmental hurdles, surpassing LFTs, is yet to be seen.

CFTs differ from LFTs insofar as CFTs directly capture fingerprint images without physical contact to a collection medium or sensor; hence, the use of the term ‘contactless’ to describe the technologies. LFTs, which include ink and optic contact based methods, rely on some sort of direct contact with a capture medium or sensors to generate fingerprint images. LFTs rely on some sort of physical medium, such as ink, paper, or plate, or direct physical contact with a sensor to capture users’ fingerprint images. The conception of what constitutes CFTs occupies a spectrum to include technologies where no contact with a device is required to those that require contact with a device but not a sensor.^{xx}

CFTs represent the third major generational advancement in fingerprint collection techniques. Historically, the first technique used to collect fingerprints was ink and paper. Ink is used to capture the tops of fingerprint ridges on paper after pressure is applied. The second technique

developed to collect fingerprints was optics based. Optics based fingerprint collection techniques capture light reflected from the tops of fingerprints on a plate to capture fingerprint images. Both of these techniques require users to make physical contact with some sort of collection medium whether it is ink and paper or plate. The third fingerprint collection technique developed are contactless methods. CFTs use various sensors to image users' fingerprints and do not require users to contact the collection medium or sensor.^{xxi}

Advantages of Contactless Fingerprint Technologies

CFTs afford certain potential advantages over LFTs. CFTs offer the following potential advantages to LFTs: faster capture times, unattended operations, and more hygienic. These advantages are marked over LFTs should they fully manifest as CFTs mature. However, CFTs are in their infancies, and these advantages are not yet necessarily fully realized.^{xxii, xxiii}

CFTs, unlike LFTs, can capture three dimensional images of users' fingerprints directly without the use of a flat surface or physical contact with sensors. Contrariwise, LFTs rely on users pressing their three dimensional fingers on two dimensional surfaces, which yields some distortion in the captured image. CFTs direct sensing and collection methods mitigate this problem as well as other problems such as inappropriate ink amounts and surface contamination and provide truer fingerprint images.^{xxiv, xxv}

CFTs potentially capture users' fingerprints and process higher volumes of users more quickly than LFTs. CFTs direct collection methods do not require inking and can operate without an attendant. These factors potentially allow CFTs to improve processing times in high volume locations and save operators money in regards to staff and training compared to those associated with LFTs.^{xxvi, xxvii}

CFTs potentially provide, by their very nature, more hygienic alternative to LFTs. With CFTs, users do not come into physical contact with a collection medium like ink, paper, or plates that others have touched. As a result, CFTs inhibit the transmission of pathogens from person to person.^{xxviii, xxix, xxx}

Iris Technology

The current state of contactless iris biometric technology focuses on identification and authentication of travelers, financial transactions, and infrastructure security. Contactless Iris biometric technology consists of taking an image capture of an individual's iris for enrollment in a government or private sector company's repository. Then, this individual's iris is captured or scanned again to authenticate or verify the individual's identity.^{xxxi}

Federal Government entities utilizing contactless Iris recognition technology include the US Department of Homeland Security's (DHS) Customs and Border Patrol (CBP). In 2015 in early 2016, CBP began capturing biometric, including Iris biometrics, at the Otay Mesa border crossing: "The CBP began screening certain foreign nationals entering the country via the port of entry on Paseo Internacional in December [2015]. CBP officials said biometric exit testing at the border's pedestrian crossing was an extension of the inbound phase of the project. The biometric data will be garnered from travel documents at recently installed kiosks identical to those used for inbound processing."^{xxxii} While these Iris biometric pilot programs have great potential, the US federal government lacks a robust, mature repository of captured Iris images for dependable identification and authentication.^{xxxiii} Furthermore, other government entities such as the United Nations and the Indian Government have incorporated contactless Iris recognition technology in their international or national identification strategies.^{xxxiv}

Additionally, state and local agencies used and initiated pilot programs for border security, and correctional facility identification and verification of inmates. The New York Police Department used hand-held scanners to capture iris images of criminals dating back to 2010^{xxxv}, while the El Paso Police Department decided in April 2017 to use technology that "combines iris-scanning with fingerprint- and facial-recognition capabilities, with the goal of increasing border security and weeding out criminals".^{xxxvi}

Private sector companies have also used Iris recognition technology for access control and emerging technologies. Google has implemented Iris recognition technology to verify individuals' identities in data centers^{xxxvii}, Microsoft had added this technology to Lumia phones^{xxxviii}, and Samsung worked with Princeton Identity and its patented iris recognition technology to create the first iris scanning technology available on a smartphone that gives users the ability to verify financial transactions with 'Selfie Pay'.^{xxxix-xl}

Section 2: Limitations and Challenges

Not surprisingly, this heavy use of biometric technology or software by law enforcement, as well as other homeland security entities and even the private sector, has generated significant concerns regarding the limitations, validity, and even the legality of these systems.

Face Recognition

Although the technology has come a long way over the years and error rates have continued to decline^{xli}, facial recognition systems are still not 100 percent accurate^{xlii}, and as with any type of investigative tools, accuracy is paramount. Given that the human face changes in shape and texture over time, facial recognition technologies must be robust enough to changes that are created from the aging process, as this is a current source of higher error rates in current facial matching systems. Other sources of errors in face recognition technology may be attributed to variations in pose, illumination of the face, and expression, as well as other factors including

image quality (e.g. resolution, blur). Studies have also shown that individuals of certain demographics may register errors in facial matching results more often^{xliii}, and even wearing glasses can result in higher error rates for unfamiliar face matching.^{xliiv} In 2010, National Institute of Standards and Technology (NIST) looked into and reported on the accuracy of face identification algorithms. As part of that study, NIST found that, when using the most accuracy face recognition algorithm available among those developed by seven commercial providers, they were able to accurately identify a single unknown individual in a database of approximately 1.6 million criminal records 92 percent of the time. When the range of top-matching candidates was increased to 50 for the same pool, the accuracy increased to 97 percent of the time and in cases where the top 200 candidates were searched, the correct match was found 97.5 percent of the time.^{xliv}

Past tests that the FBI has conducted for its own NGI facial recognition solutions came up with an 85 percent accuracy rate, although the FBI has acknowledged that this technology is only used as an investigative lead, and not as a means of positive identification.^{xlvi} At major airports throughout the country, DHS has been testing, and following relative success of these tests, implementing new biometric recognition solutions for one-to-one verification purposes at exit gates for international travelers. Yet despite the success of these tests within the past year, there is still the potential for identity checks to fail, as something as simple as a smile at the gate could trigger a mismatch when compared to a serious expression provided in a passport photo^{xlvii}, an issue has been identified as a continuing source of error rates for many facial recognition programs.^{xlviii} In addition, face recognition technologies on the whole are in general less accurate than fingerprinting, especially when used in on large databases or in real-time situations during law enforcement-related investigations.^{xlix}

As government agencies and commercial entities consolidate biometric data in databases, especially personal identifiers that cannot change, there is concern that they need to scrutinize closely how they implement their use. As databases are created to store Personal Identifying Information (PII) biometric information and government agencies use it more and more, these databases are now targets and the risk for data breaches increase. The privacy rights organization, Electronic Privacy Information Center (EPIC) has urged TSA to consider options for expanding the collection of biometric identifiers for the TSA Pre-Check application. EPIC draws concerns on the dangers of biometric identifiers being used for purposes other than determining eligibility for Pre-Check, calling attention to the rising potential for mission creep. In addition, the concerns raised focused on proper collection, storage and deletion when necessary of biometrics for Pre-Check applicants.^{lii} Ultimately for TSA and government use the technology is available but the limitation of expansion may be focused on what funding is available and challenges of privacy of personal identifiers in US laws and regulations of government agency use and public perception and response.

States may have different privacy laws on the books regarding how public institutions use facial recognition technology or software. For example, in May 2017, a facial recognition system being

utilized by Vermont's Department of Motor Vehicle was suspended after the state's attorney general determined that the system was in violation of a state law passed in 2004 that expressly prohibited the DMV from using biometrics, following similar findings by the Vermont chapter of the American Civil Liberties Union. Vermont's DMV had been using the facial recognition system to search through its records.^{lii}

Some states have also targeted the use of biometric technologies by companies such as Facebook or Google. Illinois's law, the 2008 Illinois Biometric Information Privacy Act ("BIPA"), prohibits companies from collecting the measurements of any individual's biological features without the individual's consent. Illinois defines a "biometric identifier" as: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry". Photographs, writing samples, demographic data, and physical descriptions are excluded from this definition. However, courts have consistently found that a photograph can be converted into a "scan of ... face geometry" if software uses the measurements and structure of a face to uniquely code or identify it. Facebook^{liii}, Shutterfly^{liv}, and Google^{lv} have all been sued under the Illinois BIPA because their face recognition technology enables photographs of a person's face (and the "face scan" that can be created from it) to be used to identify persons in other photographs. The plaintiffs claim that their rights have been violated under the BIPA because their consent was not obtained to enable their photographs to tag photos with personal identifiers. The plaintiffs described Facebook as having "secretly amassed the world's largest privately held database of consumer biometric data."^{lvi} These cases are currently making their way through the courts.

Texas (2009) and Washington State (2017) have passed their own biometrics laws. Under the Texas law, only the attorney general can sue, not individuals. The Washington State law is similarly limited to the State Attorney general and allows companies to use fingerprints, eye scans and facial photographs.^{lvii} At a federal level, the Federal Trade Commission provides best practices guidelines, but there has been no federal legislation in this area. The Washington State law exempts images that are already online from its scope. However, many companies that are developing new biometric programs for their products and services, are pushing back on proposals for such laws at the state level, and eight other proposals in states have not passed due in part to lobbying efforts by companies with stakes in biometric technology development and use. Companies argue that such laws may encourage fraud if businesses avoid developing and utilizing biometric software and data for fraud detection and verification purposes in their products and services out of concerns for the risk of costly class action lawsuits.^{lviii}

In India, the Indian Supreme Court is currently hearing challenges to the Aadhaar identity system. Petitioners have claimed that the Aadhaar system makes too many private transactions visible to the state and that private data is not adequately safeguarded.^{lix}

More speculatively, in the "Nosedive" episode of the online show *Black Mirror*,^{lx} a near-future scenario is presented in which embedded face recognition technology enables participants in a private, voluntary system reinforced by social norms, to identify and see the background of other

participants they encounter in public at all times. Because semi-anonymity in public is lost, citizens rigidly conform to very high standards of public behavior because their identity is linked to a reputation score that is constantly up- or downgraded by people they encounter. While not based on face recognition, this is similar to an actual system rolled out in China that rewards valued behaviors with increased credit ratings.^{lxi} The Nosedive episode does draw attention to our assumption that we can largely be semi-anonymous in public situations. To what extent is this a right?

Biometric identification systems still require mostly controlled contexts to do verification or identification of subjects: participant must pose in front of special cameras looking directly into the camera and so on. Technically, it is far from possible to identify faces in uncontrolled environments at a large scale reliably.^{lxii} Iris scans and contactless fingerprints are similarly highly constrained.

As governments also continue testing and implementing biometric identity solutions with the goal of enhancing security around the nation, concerns have also arisen that the gathering and management of facial identify data will be used to violate the civil rights and liberties of both immigrants and citizens alike. In the United States, nonimmigrant foreign visitors to the country have been required by law since 2004 to submit to fingerprint and photo identity scans prior to entry.^{lxiii} With the testing of biometric face-scanning technology at Dulles International in the Washington, D.C. area, and the implementation of the program at five other major United States airports, concerns have arisen from privacy protection advocacy groups that government agencies such as the DHS are stepping over legal boundaries in tracking and collecting biometric data on passengers to and from the United States. While the program that has been implemented at Dulles and other airports does not retain scanned images of US citizens, some regard the program as overstepping DHS's authority granted by the 2004 law given that all individuals boarding international flights are scanned, not just foreign nationals.^{lxiv} Representatives from the American Civil Liberties Union argue that making facial scans mandatory at exit points for even US citizens pushes the country further towards a state in which pervasive surveillance measures allow local, state, and federal law enforcement to track citizens wherever they go.^{lxv} Even now, it is estimated that half of all adult Americans—more than 117 million people—are in law enforcement facial recognition databases, and only one of 52 agencies that acknowledge use of facial recognition technologies had received legislative approval for use of these technologies.^{lxvixvii}

Overstepping by law enforcement and the government are not the only concerns that have arisen surrounding the use of facial recognition systems, commercial entities have also come under the same suspicion. Privacy advocacy organizations have reported that the information collected through facial recognition systems by commercial entities at their respective venues may be sold or shared without the consent of the individual whose image is captured and stored. The data that comes from facial recognition systems could be particularly useful to commercial entities as they could potentially identify and link to an individual's online presence, allowing for even

greater targeted advertising abilities.^{lxviii} While this ability to track and anticipate the needs and wants of consumers is certainly valuable to the private sector, the privacy concerns that this raises are certainly enormous and worthy of consideration.

Contactless Fingerprint

The developing status of CFTs leaves standardization practice in flux. The NIST issued the Cooperative Research and Development Agreement in January 2015, to “produce open testing methods, metrics and artifacts” of contactless fingerprint capture.^{lxix} As an emerging technology, standards cannot be fully measured since the program is ongoing.

CFTs creates a new data source of human identification requiring management and oversight to ensure against nefarious actors. An impersonal collection method does not necessarily trigger the owner’s recognition of a biometric record creation. Storage requirements can vary by region or sector and donors have limited control over the use of their information once it is captured. Both government and private sector engaging CFT for identity verification and security, possess a great responsibility to properly manage the output data to ensure against abuse.

Although CFTs afford certain advantages over LFTs, they also present an array of disadvantages. These disadvantages are intimately tied to CFTs’ overall newness; consequently, these disadvantages are best described as developmental hurdles. CFTs do not readily work with biometrics infrastructures already in common use by the government, law enforcement, and military nor do they capture nail-to-nail (N2) fingerprint images. Further, the public is not widely familiar with CFTs and inexperienced with how to operate such technologies properly. The further development of CFTs may overcome some or all these and related developmental hurdles.^{lxx, lxxi}

Unlike LFTs, CFTs do not widely meet or exceed government certification standards for fingerprint biometric collection systems. These standards set guidelines for fingerprinting technologies’ performance and capabilities as well as their interoperability with legacy government biometric systems and databases. No CFTs are certified at the government’s highest standard: Appendix F, which is highly concerned with one-to-many fingerprint identification and systems

US Government Fingerprint Biometric Collection Systems Certifications

The US Government certifies fingerprint biometric collection systems based on two standards.

- Appendix F has stringent image quality conditions, focusing on the human fingerprint comparison and facilitating large scale machine many-to-many matching operation.
- PIV-071006 is a lower-level standard designed to support one-to-one fingerprint verification. Certification is available for devices intended for use in the FIPS 201 PIV program.

“IAFIS FAQs.” *FBI Biometric Specification*. FBI Biometric Center of Excellence. Web. 27 Jul. 2017.

interoperability. Two CFTs are certified to the government's lower standard, PIV-071006, for one-to-one fingerprint identity verification matching; however, they are certified with caveats due to their interoperability limitations with certain government legacy biometric systems and databases. CFTs' overall lack of government certifications is reflective of interoperability issues with legacy infrastructure.^{lxxii, lxxiii, lxxiv, lxxv}

Fingerprint Identification Methods

One-to-One: This method confirms a user is who they claim to be. This is done by a device obtaining a user's fingerprint and comparing it only against a retained fingerprint attributed to the user in a database. Its intended use is identity verification.

One-to-Many (including Many-to-Many): This method checks submitted fingerprints against all fingerprint records in a database. Its intended use is identification.

Thakkar, Danny. "Fingerprint Verification vs Fingerprint Identification." *Touch N Go*. Touch N Go, 11 Feb. 2016. Web. 2 Aug. 2017.

CFTs generate fingerprint images in fundamentally different formats than those generated by LFTs which leads to interoperability issues with legacy government biometric systems and databases. CFTs capture fingerprint images with varied sensors and in multiple formats. Some of these formats include true three dimensional representations of fingerprints while others imitate three dimensional captures through other means. Legacy government biometric systems and database are not designed to accommodate and process the varied outputs CFTs generate. As a result, CFTs are deficient to LFTs in regards to overall usability. Currently, CFTs are at risk of developing into "walled gardens" that do not interact with legacy government biometric systems and databases.^{lxxvi, lxxvii}

CFTs are also, currently, unable to collect true nail-to-nail (N2N) fingerprints. N2N fingerprinting captures a person's entire fingerprint from one edge of the nail bed to the other including the sides and bottom. As a result, N2N fingerprint images are very useful for fingerprint matching and identification. Current CFTs inability to capture true N2N fingerprints represent significant developmental hurdle given the importance of N2N fingerprint images in fingerprint matching and identification.^{lxxviii, lxxix}

CFTs, potentially, capture and process users' fingerprints at a pace faster than LFTs and in a more hygienic fashion. However, CFTs still face developmental hurdles in these respects due to human misuse. CFTs are new to the general public. This means users can be unfamiliar with CFTs' correct functionality and lead to their misuse. Misuse can lead to slower fingerprint processing times, unneeded physical contact with scanning apparatuses, and lower end-user satisfaction – all of which undermines CFTs' processing speeds and hygienic advantages over LFTs. As a result, some users can find LFTs easier to use and preferable to CFTs.^{lxxx, lxxxi, lxxxii}

Iris Technology

Even with contactless iris biometric technology in its relatively nascent biometric maturity, privacy, accuracy, and security limitations and challenges exist. As with other contactless biometric technologies, people have privacy concerns surrounding the necessity of having one's eye scanned and image captured for identification and verification. Who will capture this (PII)? Who will store Iris images and will this data be in a centralized or decentralized repository? These privacy and standardization questions are raised by not only individuals but also by civil rights groups. In India, civil rights groups have questioned and challenged the Aadhaar biometric system, the Indian government's country-wide biometric identification system, which includes Iris biometric capture.^{lxxxiii} Taxpayers in India must have an Aadhaar Number and a permanent account Number (PAN). If they do not have an Aadhaar Number, their PAN would be invalidated. If this limitation occurred, India's citizens' ability to buy car or utilize financial accounts could be impeded.^{lxxxiv}

Additionally, hacking, distance between an individual and the iris scanner, glare from wearing glasses^{lxxxv}, scaring over the iris, and age are challenges moving forward for contactless biometric technology. Hackers have exploited products that utilize contactless iris capture as they were able to gain entry into the Samsung S8 Iris scanner creating concerns about the security of the Iris capture for Samsung's smartphone.^{lxxxvi} Age can impact capturing clear and effective Iris images. Young children, especially infants, may have their eye closed during iris capture. A young child would need to have their Iris image captured with other PII in order to ensure positive one to one matches.

Furthermore, balancing biometric capture versus one's privacy is challenging. States such as Washington, Texas, and Illinois have passed privacy laws ensuring legal protection for their citizens against excessive biometric capture. Washington State's law, H.B. 1493, which went into effect July 23, 2017, stipulates that "A person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose [. . .] Unless consent has been obtained from the individual, a person who has enrolled an individual's biometric identifier may not sell, lease, or otherwise disclose the biometric identifier to another person for a commercial purpose. . ."^{lxxxvii}/^{lxxxviii} Despite only three US States having passed privacy laws, more states will likely consider legal protections for their citizens against biometric capture technology.

Section 3: Future State of Biometrics

Face Recognition

As facial recognition systems become more accurate, their use will become much more prevalent. Many local police departments are currently exploring the utility of real-time face recognition on live surveillance video, allowing them to scan the faces of individuals walking within the view of a street surveillance camera.^{lxxxix} On the commercial side, experts predict that facial recognition systems will help industry leaders to improve marketing and customer service through more targeted, customized messaging, products and services.^{xc} Some systems are already being used in digital advertisements—typically televisions or kiosk displays in stores—which contain cameras that recognize certain characteristics of the advertisement’s viewer, such as their gender or age, and then target advertisements accordingly and in real-time based on this information. In the future, facial recognition technologies used by retailers to identify returning customers by name and further target advertisements toward specific individuals based on their past purchases or other available information.^{xci}

In the near future, biometric verification of government-enrolled identities can provide real convenience in scenarios such as travel, where face recognition for boarding passes has been accepted quite readily.^{xcii} Conversely, private use of decentralized, private biometrics can provide increased security, an improvement over centralized password stores that can be hacked into or guessed, and can also be used by retailers to identify returning customers by name and further target advertisements toward specific individuals based on their past purchases or other available information.^{xciii} Facial recognition technology has achieved near-human levels of accuracy in controlled environments, using human verification as a fallback can speed processes up, as long as the machine matching of faces is on the order of seconds.

Ideally, the future of facial recognition biometrics is one which properly balances superior accuracy with the need for maintaining privacy protections of any individual in range of a facial recognition system. As these systems become more accurate and more widely used by companies and governments, new legislation may be necessary to ensure that privacy and PII is properly protected and that civil rights and liberties are not infringed upon. In 2016, Georgetown University’s Center on Privacy & Technology released a report on the use of biometric facial recognition systems by law enforcement agencies around the country, as well as a list of recommendations for legislation to regulate this use, including limiting mug shots (not driver’s license and ID photos) to be the default photo in face recognition databases and requiring searches of license and ID photos by court order issued upon a showing of probable cause.^{xciv} These recommendations also includes calls for accuracy and bias testing by law enforcement agencies through independent testing to determine not only the overall accuracy of the facial recognition system being used, but also whether or not that system is in any way varies or is less accurate based on race, ethnicity, gender, or age.^{xcv}

Our panelists—at the MIT Working Session on July 24, 2017—suggested that within seven years, we can expect to see seamless end-to-end traveler verification via biometrics, increased consumer/personal control of personal data, the complete transformation of identity systems to digital identity systems, and the merging of biometric identifiers with cars, home systems and the Internet of Things.

Going forward, as people become increasingly conscious of their right and responsibility to maintain their digital identities, including their biometric identifies, Prof. Sandy Pentland at the MIT Media Lab, believes that people will increasingly expect a “New Deal on Data”. Under this New Deal,

1. You have a right to possess your data. Companies should adopt the role of a Swiss bank account for your data. You open an account (anonymously, if possible), and you can remove your data whenever you’d like.
2. You, the data owner, must have full control over the use of your data. If you’re not happy with the way a company uses your data, you can remove it. All of it. Everything must be opt-in, and not only clearly explained in plain language, but with regular reminders that you have the option to opt out.
3. You have a right to dispose or distribute your data. If you want to destroy it or remove it and redeploy it elsewhere, it is your call.^{xcvi}

The Media Lab has converged on 5 principles to guide digital identity architectures.

1. Contractual adjustable control over (personal) data by all stake holders
2. Security of Identity, data and transactions
3. Minimized data sharing with trust and local computation
4. Total encryption (data at rest and in transit)
5. Matching technical architecture with legal governance models.^{xcvii}

These principals can help people maintain control over their digital identity. For details and early implementations of these ideas, see [MIT's TRUST::DATA Consortium](#) projects.

Contactless Fingerprint

The proliferation and maturation of CFTs in the public and private spheres is likely given the potential benefits. The potential benefits to both user types are profound. In the near term, developmental hurdles associated with CFTs will likely be overcome – especially those associated with public familiarity and processing times due to increased public exposure. In the medium to long term, developmental hurdles related to CFTs lack of certified interoperability with legacy government biometric systems and databases will be overcome. Further, as part of the government certification processes, CFTs will also support all fingerprint matching techniques to include one-to-one, one-to-many, and many-to-many. Additionally, privacy concerns over ‘big brother’ collection, privacy, and lack of precedence since CFT standards are still in development creates a challenging legal landscape, but public policy solutions will likely develop over time to address these concerns. Users must trust in sound policies, despite hackers proving once-thought

impenetrable networks vulnerable. Societies must undergo these growing pains to forge new technological territory. All considered, CFTs represent a major step forward in respect to biometrics and identify information. CFTs will develop into a major asset to the public and private spheres in the United States and world-wide in respect to biometrics and identity information to include all areas where such information is relevant.

Iris Technology

While privacy, accuracy, and standardization challenges inhibit contactless Iris biometric technology, the future has vast opportunities for public, private, and military use, including Investigative use. Capturing Iris biometrics during traffic stops can safeguard law enforcement officers' physical security and improve investigative tactics.^{xcviii}

Similarly, the US military seeks iris biometric technology to assist their field operations' in real time and their investigative abilities with military headquarters entities: "Embedded with Iris ID's R-100 camera and IrisAccelerator, CATS [Combat Apps Tactical System] enables front-line operatives to capture biometric data for authenticating troop identities in real time using intelligence databases stored securely and remotely at the mission headquarters. Military can also use the iris recognition capabilities to verify troop identities before boarding ships, airplanes or other types of transportation."^{xcix}

Additionally, the healthcare industry may incorporate contactless Iris biometric technology for managing health care applications that identify patients and verify insurance information. Ideally, use of iris biometric technology will reduce fraud and streamline the patient experience while they receive healthcare.^c

Despite the military, health, and private entities strategies to increase Iris recognition technology, will the average consumer desire this biometric over other traditional biometrics (fingerprint), or continue using standard passwords for securing their data? Polling data suggest that individuals desire more biometrics, potentially including Iris technology: "Seventy-nine percent of respondents said they wanted to be able to use biometric modalities beyond fingerprint scanning to access mobile payment or banking apps, and 42 percent said they wouldn't use any such apps if they weren't secured with biometric authentication. Eighty-six percent said that biometric authentication is easier than password-based login."^{ci}

Finally, iris recognition may assist with airport and major event security, which has become an increased concern with Islamic State of Iraq and ash-Sham (ISIS)-inspired individual conducting attacks, including attack such as May 22, 2017 attack after the Ariana Grande concert in Manchester, England. Clear, an Iris biometric technology company, has implemented kiosks at major US airports and sporting events.^{cii} Even though this technology is mostly at airports, the

technology will likely mature and may expand at major sporting events and potentially concerts at these sporting event locations, leading to increased security for US citizens.

Conclusion

According to a Carnegie Mellon Study, none of the challenges that Biometric Facial Recognition are “systemic”: ultimately, over time, research in biometrics has been and will keep overcoming every challenge. Social Networks are growing their databases of people’s faces every day and algorithms are getting better at distinguishing between similar faces, and computing continues to get cheaper. From the technological perspective the ability to successfully conduct mass-scale facial recognition is inevitable according to the Carnegie Mellon study.^{ciii} Biometrics is in our future. The question will be can government agencies keep up with the private sector abilities. Additionally, as Prof. Pentland at MIT told us, smartphones already log an incredible amount of biometric data, location data, and information about a person’s pattern of life that can be used to identify who is using them with very high reliability.

During the course of our research, we found several systems in which private companies leverage publicly collected biometrics (largely, face recognition biometrics derived from identification photos for passports or driver’s licenses). We did not see any instances of public, governmental organizations using privately collected biometrics, although government agencies can subpoena information, including images from online social networks.^{civ} Only governmental agencies, it seems, have the ability to reliably enroll large numbers of participants with biometric identifiers, as we have seen with the Indian government’s Aadhaar program, the US government’s use of passport and visa photos, and some states’ enablement of API verification of driver’s license information.

Private company use of private biometric data, such as Facebook’s identifying persons in photographs on the basis of previously identified faces, and Hypr’s decentralized biometric authentication system for access to online banking and other services is limited. In the authentication scenario, access is secure, since the biometric is stored on the user’s own cell phone, but participation is voluntary and limited. In the case of photo-tagging systems like Facebook, coverage is wide, but because the enrollment system is not controlled—it is based entirely on participants associating names with faces in photographs—it can easily be spoofed. Until private companies can reliably enroll large numbers of people biometrically in their systems, private use of privately-enrolled biometrics will be very limited. The risk of theft of private biometric data poses a huge risk for private companies.

Finally, as we saw with the working systems whose representatives we interviewed, the system must verify that the person presented is living—through motion or other biometrics—before the identification can be trusted. Systems providers must ensure that it is not possible to spoof a biometric identification system with a static photograph or fingerprint.



Acknowledgements:

We would like to thank Daniel “Dazza” Greenwood, Visiting Scientist in Computational Law Research and Development at the MIT Media Lab’s Human Dynamics Lab, for organizing the Digital Identity Working Session on July 24, 2017, in which we took part, as well as all the other participants, as well as the Human Dynamics Lab director, Prof. Alexander “Sandy” Pentland, of MIT, who made time to meet with us.

-
- ⁱ United States. Government Accountability Office. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*. Web. <http://www.gao.gov/assets/680/671764.pdf>, pg. 3
- ⁱⁱ Lawrence, Steve, et al. "Face recognition: A convolutional neural-network approach." *IEEE transactions on neural networks* 8.1 (1997): 98-113.
- ⁱⁱⁱ United States. Government Accountability Office. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*. Web. <http://www.gao.gov/assets/680/671764.pdf>, pg. 10
- ^{iv} Center for Democracy & Technology. "Seeing is ID'ing: Facial Recognition & Privacy" *Center for Democracy and Technology*, 2012, pp.1, Accessed May 26, 2017. pp. 4
- ^v Lachance, Naomi. "Facebook's Facial Recognition Software is Different From the FBI's. Here's Why." *NPR*, 18 May, 2016, <http://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why>
- ^{vi} "Amazon Rekognition" amazon web services, <https://aws.amazon.com/rekognition/>. Accessed 6 July 2017.
- ^{vii} "Apple developing 3-D face scanning feature to unlock upcoming iPhone." *BiometricUpdate.com*, 4 July 2017, <http://www.biometricupdate.com/201707/apple-developing-3-d-face-scanning-feature-to-unlock-upcoming-iphone>
- ^{viii} United States. Government Accountability Office. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*. Web. <http://www.gao.gov/assets/680/671764.pdf>, pg. 9
- ^{ix} Braga, Matthew. "Facial recognition technology is coming to Canadian airports this spring." *CBC News*, 6 Mar. 2017, <http://www.cbc.ca/news/technology/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344>
- ^x Braga, Matthew. "Facial recognition technology is coming to Canadian airports this spring." *CBC News*, 6 Mar. 2017, <http://www.cbc.ca/news/technology/cbsa-canada-airports-facial-recognition-kiosk-biometrics-1.4007344>
- ^{xi} United States. Customs and border Protection. *1-to-1 Facial Comparison Project*. Web. <https://www.cbp.gov/sites/default/files/documents/502745%20-%201%20to%201%20Face%20ePassport%20for%20JFK%20-%20FACT%20SHEET%20-%20FINAL%20%28web%20ready%29.pdf>
- ^{xii} CBP has been working with our stakeholders to build a simplified but secure travel process that not only meets the biometric exit mandate, but also aligns with CBP's and the travel industry's modernization efforts," said John Wagner, CBP's deputy executive assistant commissioner for field operations.
- ^{xiii} "Face scans for Americans flying abroad stir privacy issues." *Associated Press*, 12 July 2017, <https://apnews.com/493bb45a827f483e84f00a22000c96cb>
- ^{xiv} Wisniewski, Mary. "At O'Hare, some passengers undergo face scans in test of security program." *Chicago Tribune*, 20 July 2017, <http://www.chicagotribune.com/news/local/breaking/ct-face-scans-ohare-0720-20170719-story.html>
- ^{xv} NBC News. "JetBlue Tests Facial Recognition Technology". June 16, 2017. <http://www.nbcnews.com/nightly-news/video/jetblue-tests-facial-recognition-technology-969580099532>
- ^{xvi} Gabriele Parussini. India's Digital ID Rollout Collides With Ricketty Reality. *Wall Street Journal*, January 13, 2017. <https://www.wsj.com/articles/snags-multiply-in-indias-digital-id-rollout-1484237128?mg=prod/accounts-wsj>
- ^{xvii} "For the current population of 1.2 billion the expected proportion of duplicands is 1/121, a ratio which is far too high." Hans Verghese Mathews, *Flaws in the UIDAI Process*. *Economic & Political Weekly*. Vol. 51, Issue No. 9, 27 Feb, 2016
- ^{xviii} Del Greco, Kimberly J., "Law Enforcement's Use of Facial Recognition Technology." *FBI*, 22 March 2017, <https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology>
- ^{xix} Garvie, Clare, Alvaro Bedoya, Frankle, Jonathan. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." *Georgetown Law Center on Privacy & Technology*, 18 Oct. 2016, <https://www.perpetuallineup.org/>
- ^{xx} Wiggin, Phillip, and Lars Ericson. *Contactless Fingerprint Technologies Assessment (Version 2)*. Department of Justice, 7 Feb. 2014. PDF. 2 Aug. 2017. <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf> <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf> <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf>

- ^{xxi} Garris, John, and John Libert. "NIST Contactless Fingerprint Metrology Project." 11 Aug. 2016. Microsoft PowerPoint file. 1 Aug. 2017. <https://www.nist.gov/document/iai2016-nistcontactlessfingerprints-distro-20160811pdf>
- ^{xxii} Wiggin, Phillip, and Lars Ericson. Contactless Fingerprint Technologies Assessment (Version 2). Department of Justice, 7 Feb. 2014. PDF. 2 Aug. 2017. <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf>
- ^{xxiii} Jontz, Sandra. "Touchy Subject : NIST Works to Verify Contactless Fingerprint Technology." Signal. AFCEA International, 10 Sep. 2015. Web. 2 Aug. 2017. <https://www.afcea.org/content/?q=Article-touchy-subject-nist-works-verify-contactless-fingerprint-> <https://www.afcea.org/content/?q=Article-touchy-subject-nist-works-verify-contactless-fingerprint-technology>
- ^{xxiv} Wiggin, Phillip, and Lars Ericson. Contactless Fingerprint Technologies Assessment (Version 2). Department of Justice, 7 Feb. 2014. PDF. 2 Aug. 2017. <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf>
- ^{xxv} Jontz, Sandra. "Touchy Subject : NIST Works to Verify Contactless Fingerprint Technology." Signal. AFCEA International, 10 Sep. 2015. Web. 2 Aug. 2017. <https://www.afcea.org/content/?q=Article-touchy-subject-nist-works-verify-contactless-fingerprint->
- ^{xxvi} Wiggin, Phillip, and Lars Ericson. Contactless Fingerprint Technologies Assessment (Version 2). Department of Justice, 7 Feb. 2014. PDF. 2 Aug. 2017. <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf>
- ^{xxvii} Jontz, Sandra. "Touchy Subject : NIST Works to Verify Contactless Fingerprint Technology." Signal. AFCEA International, 10 Sep. 2015. Web. 2 Aug. 2017. <https://www.afcea.org/content/?q=Article-touchy-subject-nist-works-verify-contactless-fingerprint->
- ^{xxviii} Wiggin, Phillip, and Lars Ericson. Contactless Fingerprint Technologies Assessment (Version 2). Department of Justice, 7 Feb. 2014. PDF. 2 Aug. 2017. <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf>
- ^{xxix} Jontz, Sandra. "Touchy Subject : NIST Works to Verify Contactless Fingerprint Technology." Signal. AFCEA International, 10 Sep. 2015. Web. 2 Aug. 2017. <https://www.afcea.org/content/?q=Article-touchy-subject-nist-works-verify-contactless-fingerprint->
- ^{xxx} Furman, Susanne, et al. "Contactless Fingerprint Devices Usability Test." NISTIR 8171. National Institute of Standards and Technology, 6 Mar. 2017. PDF. 28 Jul. 2017. <http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8171.pdf>
- ^{xxxi} <http://www.irisid.com/productssolutions/technology-2/irisrecognitiontechnology/> (accessed August 3 2017)
- ^{xxxii} <http://www.cbs8.com/story/31202997/new-biometric-screenings-for-travelers-going-into-mexico> (accessed August 3 2017)
- ^{xxxiii} <https://www.theverge.com/2016/7/12/12148044/fbi-iris-pilot-program-ngi-biometric-database-aclu-privacy-act> (accessed August 3, 2017)
- ^{xxxiv} <https://www.ethnews.com/un-integrates-irisguards-ethereum-payment-platform-for-refugees> (accessed 11 July 2017)
- ^{xxxv} <http://www.nytimes.com/2010/11/16/nyregion/16retinas.html> (accessed August 3 2017)
- ^{xxxvi} http://www.valleymorningstar.com/news/local_news/article_3b6c91ee-1f20-11e7-963e-8b7bedb74217.html
- ^{xxxvii} <https://www.youtube.com/watch?v=cLory3qLoY8> (accessed August 3, 2017)
- ^{xxxviii} <https://www.windowcentral.com/how-iris-scanner-lumia-950-and-950-xl-works> (accessed August 3, 2017)
- ^{xxxix} <http://www.biometricupdate.com/201703/samsung-galaxy-s8-to-feature-princeton-identity-iris-technology-for-mastercard-selfie-pay>
- ^{xl} <http://www.marketwired.com/press-release/princeton-identity-iris-technology-featured-in-samsung-galaxy-s8-2206590.htm>
- ^{xli} United States. Government Accountability Office. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*. Web. <http://www.gao.gov/assets/680/671764.pdf>, pg. 5
- ^{xlii} Kramer, Robin and Kay Ritchie, "The trouble with facial recognition technology (in the real world)." *Phys.org*, 14 Dec. 2016, <https://phys.org/news/2016-12-facial-recognition-technology-real-world.html>
- ^{xliii} Klare, Brendan F., mark J. Burge, Klontz, Joshua C., Richard W. Vorder Bruegge, and Jain, anil K. "Face Recognition Performance: Role of Demographic Information." *IEEE*, 2012 <http://openbiometrics.org/publications/klare2012demographics.pdf>
- ^{xliv} Kramer, Robin S. S., "Disguising Superman: How Glasses Affect Unfamiliar Face Matching." *Wiley Online Library*, 21 August 2016, <http://onlinelibrary.wiley.com/doi/10.1002/acp.3261/full>
- ^{xlv} Grother, Patrick J., George W. Quinn, and Phillips, Jonathon, "Report on the Evaluaiton of 2D Still-Image Face Recognition Algorithms." *NIST*, 2010, http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968

- ^{xlvi} Del Greco, Kimberly J., “Law Enforcement’s Use of Facial Recognition Technology.” *FBI*, 22 March 2017, <https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology>
- ^{xlvii} “Face scans for Americans flying abroad stir privacy issues.” *Associated Press*, 12 July 2017, <https://apnews.com/493bb45a827f483e84f00a22000c96cb>
- ^{xlviii} Klare, Brendan F., mark J. Burge, Klontz, Joshua C., Richard W. Vorder Bruegge, and Jain, anil K. “Face Recognition Performance: Role of Demographic Information.” *IEEE*, 2012 <http://openbiometrics.org/publications/klare2012demographics.pdf>
- ^{xlix} Garvie, Clare, Alvaro Bedoya, Frankle, Jonathan. “The Perpetual Line-Up: Unregulated Police Face Recognition in America.” *Georgetown Law Center on Privacy & Technology*, 18 Oct. 2016, <https://www.perpetuallineup.org/>
- ^l Lee, Justin. Biometric Update “EPIC urges TSA to consider other options to expanding biometric identifiers for Pre-check” 11 July 2017, Retrieved July 20 2017 <http://www.biometricupdate.com/201707/epic-urges-tsa-to-consider-other-options-to-expanding-biometric-identifiers-for-pre-check>
- ^{li} Jansen, Bart. USA Today “Bye-Bye Boarding Pass? TSA, airlines test fingerprints, facial recognition to ID travelers” 13 June 2017, Retrieved June 30 2017 at <https://www.usatoday.com/story/news/2017/06/13/tsa-airlines-test-fingerprints-facial-recognition-identify-travelers/102812802>
- ^{lii} Dobbs, Taylor. “DMV Facial Recognition System Deemed Illegal By Vermont Attorney General.” *VPR: Vermont’s NPR News Source*, 18 July 2017, <http://digital.vpr.net/post/dmv-facial-recognition-system-deemed-illegal-vermont-attorney-general>
- ^{liii} In re Facebook Biometric Information Privacy Litigation, 185 F.Supp.3d 1155 (N.D. Cal. 2016)
- ^{liv} *Norberg v. Shutterfly, Inc.*, 1:15-cv-05351 (N.D. Ill. 2015).
- ^{lv} *Rivera v. Google Inc.*, , 2017 WL 748590 (N.D. Ill. 2017).
- ^{lvi} Kartikay Mehrotra, Tech Companies Are Pushing Back Against Biometric Privacy Laws. *Bloomberg BusinessWeek*. July 19, 2017
- ^{lvii} *Ibid.*
- ^{lviii} Mehrotra, Kartikay. “Tech Companies Are Pushing Back Against Biometric Privacy Laws.” *Bloomberg Businessweek*, 19 July 2017, <https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws>
- ^{lix} de Sam Lazro, Fred, “India’s national ID program raises privacy concerns”, *PBS NewsHour*, July 29, 2017. <http://www.pbs.org/newshour/bb/indias-national-id-program-raises-privacy-concerns/>
- ^{lx} “Nosedive”, *Black Mirror*, Series 3, Episode 1, Directed by Joe Wright, Story by Charlie Brooker, Teleplay by Michael Schur and Rashida Jones
- ^{lxi} Josh Chin and Gillian Wong, “China’s New Tool for Social Control: A Credit Rating for Everything”. *Wall Street Journal*, Nov. 28, 2016
- ^{lxii} In this video from Face-Six LLC, a Nevada face recognition company, it is demonstrated that faces detected in an online video can be matched against a series of team roster photos in near real time. <https://www.youtube.com/watch?v=-qoEmVfYME>
- ^{lxiii} “Face scans for Americans flying abroad stir privacy issues.” *Associated Press*, 12 July 2017, <https://apnews.com/493bb45a827f483e84f00a22000c96cb>
- ^{lxiv} “Face scans for Americans flying abroad stir privacy issues.” *Associated Press*, 12 July 2017, <https://apnews.com/493bb45a827f483e84f00a22000c96cb>
- ^{lxv} Khalid, Asma. “Facial Recognition May Boost Airport Security But Raises Privacy Worries.” *NPR*, 26 June 2017, <http://www.npr.org/sections/alltechconsidered/2017/06/26/534131967/facial-recognition-may-boost-airport-security-but-raises-privacy-worries>
- ^{lxvi} “Half of All American Adults are in a Police Face Recognition Database, New Report Finds.” *Georgetown Law*, 18 October 2016, <https://www.law.georgetown.edu/news/press-releases/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds.cfm>
- ^{lxvii} Garvie, Clare, Alvaro Bedoya, Frankle, Jonathan. “The Perpetual Line-Up: Unregulated Police Face Recognition in America.” *Georgetown Law Center on Privacy & Technology*, 18 Oct. 2016, <https://www.perpetuallineup.org/>

- ^{lxviii} United States. Government Accountability Office. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*. Web. <http://www.gao.gov/assets/680/671764.pdf>, pg. 16
- ^{lxix} “Contactless Fingerprint Capture,” National Institute of Standards and Technology, US Department of Commerce. N.p., 21 June 2017. Web. 28 July 2017. <https://www.nist.gov/programs-projects/contactless-fingerprint-capture>
- ^{lxx} Wiggin, Phillip, and Lars Ericson. Contactless Fingerprint Technologies Assessment (Version 2). Department of Justice, 7 Feb. 2014. PDF. 2 Aug. 2017. <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf>
- ^{lxxi} Smith, Benjamin. Personal Interview. 10 Aug. 2017.
- ^{lxxii} Certified Products List.” *FBI Biometric Specification*. FBI Biometric Center of Excellence, 14 Jul. 2017. Web. 27 Jul. 2017. <https://www.fbibiospecs.cjis.gov/certifications>
- ^{lxxiii} “Appendix F.” *Electronic Fingerprint Transmission Specification*. FBI, 2 May. 2005. PDF. 2 Aug. 2017. <https://www.fbibiospecs.cjis.gov/Document/Get?fileName=efts71.pdf>
- ^{lxxiv} “Personal Identity Verification (PIV) Image Quality Specifications for Single Finger Capture Devices.” *Biometric Specifications*. FBI Biometric Center of Excellence, 10 Jul. 2006. Web. 2 Aug. 2017. <https://www.fbibiospecs.cjis.gov/Home/BiometricSpecs>
- ^{lxxv} Wiggin, Phillip, and Lars Ericson. Contactless Fingerprint Technologies Assessment (Version 2). Department of Justice, 7 Feb. 2014. PDF. 2 Aug. 2017. <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf>
- ^{lxxvi} Wiggin, Phillip, and Lars Ericson. Contactless Fingerprint Technologies Assessment (Version 2). Department of Justice, 7 Feb. 2014. PDF. 2 Aug. 2017. <https://www.ncjrs.gov/pdffiles1/nij/grants/245147.pdf>
- ^{lxxvii} “Hands Off! NIST Helps Bring Contactless Fingerprint Technology to Market.” *NIST*. National Institute of Standards and Technology, 21 Sep. 2016. Web. 2 Aug. 2017. <https://www.nist.gov/news-events/news/2015/09/hands-nist-helps-bring-contactless-fingerprint-technology-market>
- ^{lxxviii} Smith, Benjamin. Personal Interview. 10 Aug. 2017.
- ^{lxxix} “Nail to Nail (N2) Fingerprint Challenge.” *Prize Challenges*. IARPA. Web. 10 Aug. 2017. <https://www.iarpa.gov/index.php/working-with-iarpa/prize-challenges/844-nail-to-nail-n2n-fingerprint-grand-prize-challenge>
- ^{lxxx} Furman, Susanne, et al. “Contactless Fingerprint Devices Usability Test.” *NISTIR 8171*. National Institute of Standards and Technology, 6 Mar. 2017. PDF. 28 Jul. 2017. <http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8171.pdf>
- ^{lxxxi} Stanton, Brian, et al. “Usability Testing of a Contactless Fingerprint Device: Part 1.” *NISTIR 8158*. National Institute of Standards and Technology, 7 Dec. 2016. PDF. 2 Aug. 2017. <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8158.pdf>
- ^{lxxxii} Stanton, Brian, et al. “Usability Testing of a Contactless Fingerprint Device: Part 2.” *NISTIR 8159*. National Institute of Standards and Technology, 7 Dec. 2016. PDF. 2 Aug. 2017. http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=917472
- ^{lxxxiii} <http://timesofindia.indiatimes.com/india/Learning-with-the-Times-What-is-Aadhaar/articleshow/6680601.cms>
- ^{lxxxiv} <http://www.csoonline.com/article/3194274/security/india-s-supreme-court-hears-challenge-to-biometric-authentication-system.html>
- ^{lxxxv} <http://www.iritech.com/services/faqs>
- ^{lxxxvi} <http://www.securityweek.com/hackers-defeat-samsung-galaxy-s8-iris-scanner>
- ^{lxxxvii} <http://www.focusonthedata.com/2017/07/third-state-adopts-biometric-privacy-law/>
- ^{lxxxviii} H.B. 1493 via PDF format
- ^{lxxxix} Garvie, Clare, Alvaro Bedoya, Frankle, Jonathan. “The Perpetual Line-Up: Unregulated Police Face Recognition in America.” *Georgetown Law Center on Privacy & Technology*, 18 Oct. 2016, <https://www.perpetuallineup.org/>
- ^{xc} United States. Government Accountability Office. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*. Web. <http://www.gao.gov/assets/680/671764.pdf>, pg. 9
- ^{xci} United States. Government Accountability Office. *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*. Web. <http://www.gao.gov/assets/680/671764.pdf>, pg. 9
- ^{xcii} Asma Khalid, “JetBlue Experiments With Using Your Face As A Boarding Pass”, WBUR, June 21, 2017. <http://www.wbur.org/bostonmix/2017/06/21/jetblue-facial-recognition-pilot>
- ^{xciii} <http://www.gao.gov/assets/680/671764.pdf>, pg. 9

^{xciv} Garvie, Clare, Alvaro Bedoya, Frankle, Jonathan. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." *Georgetown Law Center on Privacy & Technology*, 18 Oct. 2016, <https://www.perpetuallineup.org/>

^{xcv} "Model Face Recognition Legislation." *Georgetown Law Center on Privacy and Technology*, 18 Oct. 2016, <https://www.perpetuallineup.org/sites/default/files/2016-10/Model%20Face%20Recognition%20Legislation.pdf>, pp. 12

^{xcvi} Pentland, Alex. "Reality mining of mobile communications: Toward a new deal on data." *The Global Information Technology Report 2008–2009 (2009)*: 1981.

^{xcvii} Already a vast array of legislations cover aspects of identity and personal information. These include the Federal Privacy Act of 1974, FERPA, HIPAA, Fair Credit Reporting Act, and several others. Identity systems are not always designed with these systems in mind, with the exception of health information, regulated by HIPAA.

^{xcviii} <http://www.ibtimes.com/iris-scanners-widely-used-us-military-could-be-becoming-police-department-near-you-1917018>

^{xcix} <http://www.biometricupdate.com/201706/iris-id-technology-integrated-in-ultra-electronics-tactical-system-for-military-applications>

^c <http://www.biometricupdate.com/201706/how-government-biometrics-are-moving-into-the-private-sector>

^{ci} <https://mobileidworld.com/familiarity-biometric-login-survey-005042/>

^{cii} <http://www.biometricupdate.com/201706/clear-now-open-for-business-at-lax>

^{ciii} Meyer, Robinson. Atlantic Monthly "Who Owns Your Face?" 2 July 2015, Retrieved July 10 2017 at <https://www.theatlantic.com/technology/archive/2015/07/how-good-facial-recognition-technology-government-regulation/397289/>

^{civ} Protalinski, Emil. "Here's what Facebook sends the cops in response to a subpoena". ZDNet. April 7, 2012 <http://www.zdnet.com/article/heres-what-facebook-sends-the-cops-in-response-to-a-subpoena/>