A Closer Look: Iris Recognition, Forensics, and the Future of Privacy Note

Chantelle D. Ankerman

Follow this and additional works at: https://opencommons.uconn.edu/law_review

Recommended Citation
https://opencommons.uconn.edu/law_review/372
Note

A Closer Look:
Iris Recognition, Forensics, and the Future of Privacy

CHANTELLE D. ANKERMAN

The iris was first suggested for use in biometrically-based recognition of humans over a century ago. This notion stems from clinical observations, developmental biology, and statistical evidence that indicate the structure of individual irises is highly distinctive and stable with age. Recent technological advances have brought to the fore iris recognition systems with enhanced detection capability. The current state of the art for this powerful tool allows the capture of a moving subject's iris pattern from afar, through sunglasses, or even from a reflection. Valuable for national security and law enforcement applications, iris recognition provides a means of covert surveillance, and thus carries strong implications for constitutional and public policy concerns. Several government agencies currently employ considerable biometric databases, facilitating efficient and inexpensive tracking. Iris recognition impacts both physical and informational privacy, and should be construed as a search within the meaning of the Fourth Amendment. The regulatory gap should be addressed in a manner that weighs the benefits of security against the incursions against privacy and liberty.
INTRODUCTION .................................................................................................................. 1359
I. WHAT IS THE IRIS AND HOW IS IT “SCANNED”?
   A. THE BIOLOGY ........................................................................................................ 1360
   B. THE TECHNOLOGY ............................................................................................. 1366
      FIGURE 1: ANTERIOR AND CROSS-SECTIONAL VIEW OF THE HUMAN EYE .......... 1361
      FIGURE 2: IRIS TRANSVERSE SECTION AND CLOSE-UP ANTERIOR WEDGE .......... 1362
      FIGURE 3: HIGH-RESOLUTION NEAR-INFRARED IRIS PHOTOS ........................... 1368
      FIGURE 4: IRISCODES .......................................................................................... 1373
II. HOW CAN IRIS SCANS BE USED?
   A. IDENTIFICATION .............................................................................................. 1379
   B. SURVEILLANCE ............................................................................................... 1381
   C. SECURITY ......................................................................................................... 1382
III. IRIS RECOGNITION AND THE LAW ................................................................. 1384
   A. PRIVACY ........................................................................................................ 1385
   B. THE FUTURE .................................................................................................. 1390
CONCLUSION ............................................................................................................... 1391
A Closer Look: Iris Recognition, Forensics, and the Future of Privacy

CHANTELLE D. ANKERMAN

INTRODUCTION

The eyes are fast becoming windows to more than one’s soul. Of particular interest is the iris, the colored part of the eye that surrounds the pupil. Iris recognition is an authentication technique that falls under a branch of science known as biometrics. Biometrics is the use of technology for identification or verification of people by their physical or behavioral characteristics. Biometric systems are based on algorithms that analyze abstracted pattern representations of human characteristics, such as the iris pattern. The concept behind biometrics—human recognition by individualization of fixed measurements or physical characteristics—is not new. However, “only three of the physical characteristics and personal traits currently used for biometrics are considered truly consistent and unique: the retina, the iris and fingerprints.” Among these “high biometrics,” only the iris has the potential to surpass the retina and fingerprints in terms of speed, reliability, and accuracy in authentication—all whilst remaining non-
This is due in large part to the high degrees of randomness and immutability inherent to the structure of the iris itself. Because of the implications iris recognition technology has for national security and law enforcement, constitutional and public policy concerns need to be addressed. The purpose of this Note is to inform and equip the legal community to understand and apply this powerful tool, while preserving privacy rights.

I. WHAT IS THE IRIS AND HOW IS IT “SCANNED”?

A. The Biology

Commonly known as the colored portion of the eye, the iris is a highly vascularized and pigmented contractile structure comprised of layers of connective and muscle tissue. Figures 1 and 2 below illustrate the gross and fine anatomy of the human iris, respectively.

---

8 See id. at 104 (“Iris recognition stands out as perhaps the most ‘hygienic’ of the biometric technologies in that no part of the user’s body has to touch anything to operate the system.”). Retinal scanning is impractical as a forensic tool because it requires close physical contact with the scanning device and causes trauma to the eye. Id. at 103. Further, certain diseases can change the retinal vascular structure, which undermines the results of retinal scanning. Id. Disadvantages of fingerprint scanning include the need for physical contact, the difficulty in acquiring high quality images, and the erosion of the fingerprint over a person’s lifespan. Id. at 105.

9 See Richard P. Wildes, Iris Recognition: An Emerging Biometric Technology, 85 PROC. IEEE 1348, 1348–50 (1997) (discussing why no two people’s irises are ever the same).

10 MARTINI ET AL., supra note 1.
FIGURE 1: ANTERIOR AND CROSS-SECTIONAL VIEW OF THE HUMAN EYE**

** Rendered by Megan E.B. Foldenauer, Ph.D., CMI.
FIGURE 2: IRIS TRANSVERSE SECTION AND CLOSE-UP ANTERIOR WEDGE

Rendered by Megan E.B. Foldenauer, Ph.D., CMI.
The iris begins to form before birth, around the third month of gestation. The only internal organ that is externally visible, the iris presents a unique opportunity for biometric identification. This is because the iris contains a superfluity of randomly distributed immutable structures, which do not change appreciably over time. These complex random patterns include various identifying features such as the trabecular meshwork of connective tissue, collagenous stromal fibers, ciliary processes, arcing ligaments, radial and contraction furrows, vasculature, pits, filaments, striation, ridges, crypts, rings, freckles, a corona, and a zigzag collarette. Further, the iris pattern cannot be modified by surgery or other means without a high risk of damage to one’s vision. Together, the singularity and dichotomous anatomy of the iris render it an ideal biometrics modality: it is static, easy to detect, and difficult to counterfeit.

The iris’s individuality also results from the anomalous manner in which it takes form. The structure of the iris is not determined by one’s genetic constitution (genotype), but rather is the product of phenotype—the physical expression of features resulting from the continuous interaction of genes with the environment. Epigenetics, or genetic control by factors other than
the DNA sequence,\textsuperscript{18} can turn genes on or off.\textsuperscript{19} This extra-genetic manipulation of DNA expression explains why genetically identical twins are often phenotypically distinguishable.\textsuperscript{20} In other words, there is a continuum of genetic penetrance,\textsuperscript{21} and certain biological characteristics (like iris structure) fall on the phenotypically determined end of the spectrum.\textsuperscript{22}

According to John Daugman, considered by some to be the foremost authority on iris recognition,\textsuperscript{23} "[t]o maximize individuality, distinctiveness, and randomness, a biometric feature should be entirely epigenetic. To maximize stability over the life span . . . [it] should not change with maternal behavior produces stable alterations of DNA methylation and chromatin structure, providing a mechanism for the long-term effects of maternal care on gene expression in the offspring. These . . . gene-environment interactions during development . . . result in the sustained 'environmental programming' of gene expression and function over the lifespan . . . Epigenetic modification of targeted regulatory [DNA] sequences in response to even reasonably subtle variations in environmental conditions might serve as a major source of epigenetic variation in gene expression and function, and ultimately as a process mediating such maternal effects . . . [E]ffects on [DNA] structure . . . serve as an intermediate process that imprints dynamic environmental experiences on the fixed genome, resulting in stable alterations in phenotype."

\textsuperscript{18} Ian C G Weaver et al., \textit{Epigenetic Programming by Maternal Behavior}, \textit{7 Nature Neuroscience} 847, 852 (2004) (discussing the epigenetic effect of maternal behavior on DNA expression). The researchers further explained that


\textsuperscript{20} See Insights from Identical Twins, LEARN.GENETICS: GENETIC SCI. LEARNING CTR., http://learn.genetics.utah.edu/content/epigenetics/twins/ [https://perma.cc/M9YN-C9SG] (last visited Mar. 13, 2017) (“Because identical twins develop from a single fertilized egg, they have the same genome. So any differences between twins are due to their environments, not genetics. Recent studies have shown that many environmentally induced differences are reflected in the epigenome.”). Medical knowledge is replete with examples of phenotypic differences between monozygotic (identical) twins, among them schizophrenia and autism. Albert H.C. Wong et al., \textit{Phenotypic Difference in Genetically Identical Organisms: The Epigenetic Perspective}, \textit{14 Human Molecular Genetics} 11, 11–12 (2005).

Genetics may provide the palette, but epigenetics determines how much of each color to use in creating an individual’s portrait. \textit{Id.} at 14.

\textsuperscript{21} Genetic penetrance is defined as the extent to which a feature is heritable, or determined by genetic factors. John Daugman, \textit{Genetic Penetrance and Iris Recognition}, UNIV. OF CAMBRIDGE COMPUTER LAB., http://www.cl.cam.ac.uk/~jgd1000/genetics.html [https://perma.cc/UW7M-SQYS] (last visited Jan. 31, 2017) (“Eye colour . . . has high genetic penetrance, . . . but . . . textural details [of iris structure] are uncorrelated and independent even in genetically identical [eye] pairs.”).

\textsuperscript{22} \textit{Id.}

\textsuperscript{23} See, e.g., \textit{Interview: John Daugman, PLANET BIOMETRICS}, http://www.planetbiometrics.com/article-details/4542/desc/interview-john-daugman/[https://perma.cc/PC8A-F5JD] (June 22, 2016) ("[Daugman] is the inventor of iris recognition, and his algorithms are the basis of all public operational deployments of this biometric technology around the world.").
phenotypic development." Unlike other high biometrics, the iris meets this exacting standard. An expedient illustration of this principle is that a pair of genetically identical eyes (from a single person) has a left and right iris structure as discernable from each other as from those belonging to different individuals.

Iris structure is purely epigenetic and, once formed, remains remarkably constant over a lifetime. The iris's distinctiveness and stability have been established through two main sources of evidence: clinical observations and developmental biology. Extensive clinical studies conducted by ophthalmologists and anatomists have demonstrated that iris pattern is highly distinctive. Also, in cases of repeated observations over a subject's lifetime, iris pattern has been shown to vary little past childhood. Developmental evidence has revealed the innately random formation of iris pattern, which forecloses naturally occurring duplicates. Although the general structure and color of the iris are genetically determined, the morphogenesis of its finely detailed structure is critically dependent on environmental conditions. Developmental biology has also confirmed that a healthy iris remains mostly unchanged for life past adolescence.

These inherent physical aspects of iris structure directly bear on the iris's biometric value. Scientists and analysts objectively determine biometric efficacy in terms of "robustness and distinctiveness." The robustness of a

---

24 Daugman, supra note 21.
25 See Woodward, supra note 6, at 102-05 (discussing how both fingerprints and retinal vascular patterns, although highly unique, are subject to a large degree of alteration over a person's lifetime, while the iris remains the same). For example, fingerprints can wear down from extensive manual labor, and retinal vascular patterns can become distorted by various medical conditions, such as pregnancy, diabetes, or retinal degeneration. Id. at 103, 105, 115; see also John Daugman, How Iris Recognition Works, 14 IEEE TRANSACTIONS CIRCUITS & SYS. VIDEO TECH. 21, 21 (2004) ("[T]he ease of localizing eyes in faces, and the distinctive annular shape of the iris, facilitate reliable and precise isolation of this feature and the creation of a size-invariant representation.").
26 Daugman, supra note 25, at 24-25.
27 Woodward, supra note 6, at 103-04.
28 Wildes, supra note 9, at 1349.
29 Id.; see also John Daugman and Cathryn Downing, Epigenetic Randomness, Complexity and Singularity of Human Iris Patterns, 268 PROC. ROYAL SOC'Y LOND. 1737, 1737 (2001) (discussing the results of a study they conducted "to assess the randomness and singularity of iris patterns, and their phenotypic distinctiveness as biometric identifiers"). To accomplish this, Daugman and Downing digitized human iris images acquired over a three-year period from volunteers at kiosks throughout the United States, United Kingdom, and Japan. Id.
30 Wildes, supra note 9, at 1349.
31 Id.
32 Id. Although certain parts of the iris are formed at birth (e.g., vasculature) others (e.g., musculature) mature around two years of age, while changes in pigmentation and average pupil size continue through adolescence. Id.
33 Id. However, slight iris depigmentation and shrinking of the average pupillary opening are standard with advanced age. Id. Various eye diseases and environmental contaminants can also alter iris appearance, though these conditions are rare. Id.
34 Hoffman, supra note 2, at 45.
system is based on the false-reject rate or the probability that two data sets from the same person will not match.\textsuperscript{35} Conversely, a system's distinctiveness is measured by its false-accept rate, which is the probability that two data sets from different persons will match.\textsuperscript{36} In this manner, a biometric system's quality is normalized over a population.\textsuperscript{37} Because about 1\% of persons have an identical twin, there is a minimum false-accept rate of 1\% across a population.\textsuperscript{38} Also, the tendency for some biometric features to change over time creates a minimum false-reject rate.\textsuperscript{39} However, for iris structure, robustness is not limited by incidence of identical twins due to the lack of genetic penetrance, and distinctiveness is not limited because of the low incidence of significant alteration over a person's lifetime. Because of this ideal combination of characteristics, the iris presents a unique opportunity for biometric applications.

B. The Technology

Iris recognition works by capturing a detailed image of the iris pattern, which is then converted into a digital code and stored in a database until subsequent retrieval for comparison and matching purposes.\textsuperscript{40} Although it sounds straightforward, this process involves several fairly complicated steps. To surmount this complexity, this Section will examine the procedure in five sequential parts: 1) Scanning of the iris, also known as enrollment; 2) Conversion of the scanned iris image into a digital code; 3) Storage of the code in a database; 4) Comparison of the code with other templates previously stored in the database; and 5) An automated decision process that interprets comparison results.\textsuperscript{41}

1. Enrollment

An iris scan uses near infrared (NIR) light to detect and take a high-

\textsuperscript{35} \textit{Id.} False-reject rate, or the failure to detect a valid match, "is known as Type I error and is important in determining the accuracy of the system to a particular level of statistical significance." \textit{Id.}

\textsuperscript{36} \textit{Id.} False-accept rate, or the incorrect matching of two templates, is known as Type II error, which is "instrumental in determining the reliability of the method across a population." \textit{Id.}

\textsuperscript{37} \textit{Id.}

\textsuperscript{38} Daugman, \textit{supra} note 21. This is known as a biometric's genotypic-error rate, which undermines variability between classes. \textit{Id.}

\textsuperscript{39} \textit{Id.} This is known as the biometric's phenotypic-error rate, which increases variability within a class. \textit{Id.}


\textsuperscript{41} See Bill Siuru, \textit{Iris Recognition Systems}, 70 Elec. Now 41, 41–42 (1999) (stating that all biometric techniques involve the basic steps of enrollment, feature extraction and conversion to a mathematical code, storage as a template, and comparison with a future sample for identification or verification purposes).
resolution photo of patterns in the colored tissue surrounding the pupil.\textsuperscript{42} To capture rich details, imaging systems must resolve a minimum of seventy pixels in the iris radius, but a radius of 80–130 pixels is typical.\textsuperscript{43} Monochrome CCD\textsuperscript{44} digital cameras acquire frames of 480-by-640 pixel resolution using NIR illumination in the 700–900 nanometer wavelength band, which permits imperceptible subject imaging.\textsuperscript{45} CCD cameras contain a dense array of independent sensors, which convert incident photons into a charge proportional to the light energy detected.\textsuperscript{46} Even darkly pigmented irises reveal complex textural structure under NIR light.\textsuperscript{47} The images in Figure 3 below show the iris captured by a CCD camera using NIR light. A wide-angle camera is used to locate the eyes, and then a narrow-angle pan/tilt camera is used to acquire high-resolution iris images.\textsuperscript{48} Current iris-scanning systems can locate the iris in under a second.\textsuperscript{49} Once in focus, the image is analyzed to find the precise location of the iris's boundaries.\textsuperscript{50} Image disruption caused by pupils, eyelashes, eyelids, and reflections is corrected.\textsuperscript{51} Most glasses, contact lenses, types of eye surgery, and even blindness do not preclude an accurate iris scan.\textsuperscript{52}

\textsuperscript{42} See Daugman, \textit{Visual Recognition}, supra note 14, at 328–29 (describing iris anatomy, coloration, and pattern visualization); Wildes, \textit{supra} note 9, at 1360–61 ("The main functional components of extant iris- recognition systems consist of image acquisition, iris localization, and pattern matching.").


\textsuperscript{44} A CCD (charge coupled device) is a sensor for capturing images digitally, by converting light into an electric charge, which then creates electronic signals. \textit{What is a CCD?}, SPECTRAL INSTRUMENTS INC., http://www.specintest.com/What_Is_A_CCD.html [https://perma.cc/V9GP-3Q44] (last visited Mar. 13, 2017). "In a CCD sensor, every pixel's charge is transferred through a very limited number of output nodes (often just one) to be converted to voltage, buffered, and sent off-chip as an analog signal. All of the pixel can be devoted to light capture, and the output's uniformity (a key factor in image quality) is high." \textit{CCD v. CMOS}, TELEDYNE DALSA, http://www.teledynedalsa.com/imaging/knowledge-center/appnotes/ccd-vs-cmos/ [https://perma.cc/4FM8-UCEW] (last visited Jan. 31, 2017).

\textsuperscript{45} Daugman, \textit{supra} note 25, at 22.


\textsuperscript{47} Daugman, \textit{supra} note 25, at 22.

\textsuperscript{48} \textit{id.}

\textsuperscript{49} \textit{id.}

\textsuperscript{50} \textit{id.}

\textsuperscript{51} Wildes, \textit{supra} note 9, at 1353–54. Additionally, iris image differences resulting from image acquisition conditions, such as distance, magnification, pupil size, iris location and orientation (which depends on head tilt, eye rotation, and camera angles) can all be mathematically corrected for. Daugman, \textit{supra} note 25, at 25.

\textsuperscript{52} Adkins, \textit{supra} note 40, at 545.
FIGURE 3: HIGH-RESOLUTION NEAR-INFRARED IRIS PHOTOS

****

Reproduced with permission of Professor John Daugman, Ph.D.
The digital video camera then maps the iris using landmark features called discriminators. Although fingerprints and iris patterns are equally unique, iris scans are more reliable because they contain more discriminators. A fingerprint has about thirty-five discriminators that must match up, while an iris scan has about 260. Also, iris scanners can determine “liveness” by detecting physiological response to light and natural pupillary oscillation, which a photo cannot duplicate. Iris recognition involves multiple scans to verify that the eye is indeed moving.

Although iris scanning requires that the eye be properly positioned and held in focus, optical systems are rapidly lowering minimum image capture requirements. Current “iris-at-a-distance” and “iris-on-the-move” systems have been developed with a capture volume of nearly a cubic meter, and a capture speed of walking at one meter per second, enabling throughput rates

---

53 See supra Section 1.A (listing several identifying structural features of the iris).
54 Moo-Young, supra note 11, at 430.
55 Id.
56 Id.
57 Id.
58 Daugman, supra note 25, at 22. Because of the way iris images are encoded, even poorly focused irises cannot be confused when their phase codes are compared, whereas poorly resolved faces that look alike may be confused. Id. at 23.
of one person every second. Even though there is an upper limit to the practical range of iris scanning technology, the bottom line is that accurate images of multiple moving subjects can be captured quickly and surreptitiously from several meters away.

SRI International released its “Iris on the Move®” (IOM) technology to the public about five years ago. IOM systems work by capturing an iris image at a distance while the subject is in motion. SRI describes IOM as a fast, safe, convenient, non-invasive, nearly automatic, and high-throughput identity verification solution. The IOM technology is offered in multiple product configurations; IOM PassPort™, IOM N-Glance™, and IOM RapID-Cam II. However, the IOM PassPort product has the greatest implications for personal privacy concerns.

The SRI IOM Product Guide describes PassPort:

Ideal for high-traffic applications . . . this walk-through portal has a processing speed of 30 people per minute. Users simply walk through at a comfortable pace. The PassPort comes in an indoor or outdoor configuration. In addition to identity verification, [these] systems perform onboard subject enrollment. It is an effective solution for applications that require rapid identity verification of a large number of people.

Indeed, the common perception that iris recognition technology requires gazing directly into a scanner mere inches away has quietly become outdated. SRI now markets iris recognition as a mature technology obviating the previous need for close-up cameras, standing still for a scan, removing headgear and eyewear, and ideal image-capture conditions. SRI claims that its technology is accurate regardless of whether subjects are wearing sunglasses, and is reliable under all lighting conditions. This technology is available on the open market, and is promoted by SRI for law enforcement,

61 See id. ("[T]he need to project enough radiant light safely onto the target to overcome its inverse square-law dilution is a limitation.").
63 Id.
64 Id.
65 Id.
66 Id.
68 Id.
healthcare, and banking applications, to name only a few possible uses. Also, in 2015, SRI announced an exclusive license of IOM to Samsung for use in its mobile products. Thus, iris recognition is rapidly becoming mainstream technology, yet the general public remains largely unaware that large-scale deployment is already in motion.

2. Conversion

Once an image of the eye has been acquired, the next step is to localize the portion of the image that contains the iris. This is done through a standard machine vision technique for modeling image boundary contours, involving the use of edge detection algorithms followed by a Hough transformation. Essentially, image-processing software employs these mathematical functions to isolate the iris by mapping two circles, one at its inner boundary (between the pupil and the iris) and the other at its outer boundary (between the iris and the sclera).

69 Id. at 3–8.
72 See supra Figure 1 (indicating the location and relative positions of the iris, sclera and pupil of the human eye). The inner, pupillary boundary is relatively easy to detect, because it is generally circular and there is a striking contrast where the pupil meets the iris, whereas in finding the outer, limbic boundary, one must correct for potential eyelid obscuration of the iris. Biometric Pers. Identification Sys. Based on Iris Analysis, U.S. Patent No. 5,291,560 (filed July 15, 1991) (issued Mar. 1, 1994).
Next, further algorithms are used to compensate for image shift, scaling and rotation, conforming each newly localized iris image to the spatial alignment necessary for comparison to other templates. This family of functions was originally proposed as a framework for understanding the properties of neurons in the brain’s visual cortex. \(^7\) 2D Gabor wavelets can optimally extract information about image orientation, modulation, and position while achieving the theoretical lower limit of mathematical uncertainty. \(^6\) Because of their capacity for compact representation, 2D Gabor wavelets have become standard in computer vision image analysis. \(^7\)

Finally, polar coordinates (concentric circles and radial lines from their origin\(^7\)) are superimposed onto the localized iris image to define separate analysis zones, so that key features can be accurately located and compared in two-dimensional space. This technique corrects for changes in the iris as the pupil grows (dilates) and shrinks (constricts) in different light conditions, or due to natural oscillation. \(^8\)

The pattern of light and dark areas in the localized iris image is converted into digital form using bandpass filters (if the brightness in a given area is more than a certain threshold amount, the software registers a one, otherwise it registers a zero). \(^8\) The resulting binary code of the localized, aligned and mapped iris image is then used to generate a unique 512-digit number called an IrisCode. \(^8\) The conversion of a raw image into an IrisCode takes less than a second. \(^8\) As Figure 4 illustrates below, an IrisCode looks similar to a barcode or QR code, and is used to digitally store information.
detected about the iris pattern. Each IrisCode consists of about 5,000 bits of data.

FIGURE 4: IRISCODES

84 The iris' unique structural features are turned into a 512-digit number called an IrisCode that is then stored in a database alongside the subject's name and other information. Woodford, supra note 82.


***** Reproduced with permission of Professor John Daugman, Ph.D.
Over twenty years ago, John Daugman patented this basis for iris recognition and its underlying computer vision algorithms for image processing, feature extraction, and matching. Daugman’s algorithms have been widely licensed and after subsequent improvements, they remain the primary basis for all significant public deployments of iris recognition, although research on alternative methods continues.

3. Storage

IrisCodes can be stored on a computer database and shared among several different databases. Although IrisCodes are typically stored instead of iris images to help maintain security and privacy and may be encrypted for further protection, the risk of misappropriation is ever-present. IrisCodes have been successfully used to reverse-engineer images capable of fooling commercial iris recognition systems. Thus, some fear that a recreated iris image could allow an imposter to breach border crossings or secure facilities. However, the possibility of a replica image closely matching authentic iris images is far greater than the practicality of impersonation. Not only would a print-out of a reverse-engineered image be rather conspicuous, particularly in a manually monitored scenario, even a covertly displayed replica image (for example, printed on the surface of a contact lens) would be unable to mimic the aforementioned pupillary response to changing light and the natural oscillation reflex. These physiological features of the eye are the touchstone of an authentic iris image. With the ever-increasing sophistication and sensitivity of scanning technology, iris identity-theft remains an improbable threat.

There has also been some debate in recent years as to whether iris patterns change with age. A handful of researchers assert that they do to a

86 Daugman, supra note 74, at figs.1–16.
87 Licensing companies include IriScan, Iridian, Sarnoff, Sensar, LG-Iris, Panasonic, Oki, B12 (maintains iris code databases for the FBI), IrisGuard, Unisys, Sagem, Enschede, Securimetrics and L1, owned by Safran/Morpho. Daugman, supra note 60; Zetter, supra note 85.
88 Supra note 23 and accompanying text. The concept of iris recognition dates to 1936, but the technique did not emerge until the development of Daugman’s algorithms in the late 1980s. NAT’L SCI. & TECH. COUNCIL, BIOMETRICS OVERVIEW 1 (2006), https://www.hsdl.org/?view&did=463909. [https://perma.cc/KDS7-LU3G].
90 Zetter, supra note 85. Researchers used a genetic algorithm (which continually improves results over several rounds of data processing) to modify synthetic iris images until they matched real ones. Id. After five to ten minutes of one-hundred to two-hundred iterations, the algorithm can produce a synthetic iris image indistinguishable to a scanner from the real image. Id.
91 Id.
92 See supra Section I.B.1 ("Iris scanners can determine ‘liveness’ by detecting physiological response to light and natural pupillary oscillation, which a photo cannot duplicate.").
IRIS RECOGNITION, FORENSICS, AND THE FUTURE OF PRIVACY

statistically significant degree, while others refute their claims as confounding algorithmic failure with alteration in iris morphology. But for argument’s sake, even if irises did change appreciably over relatively short time periods (a few years, perhaps), multiple enrollments over an individual’s lifetime could easily overcome this problem. An iris template could conceivably be updated and cross-referenced with iris templates stored in other databases every time an individual is scanned.

There is also the issue of digital data corruption, a type of computer error that occurs when code is intentionally or inadvertently changed from its original, correct form. Corruption can be random and silent (i.e., undetected), and even small changes can destroy information. User error (i.e., improper file deletion or modification), malicious activity, and physical degradation of storage media are common sources of corruption. Countermeasures such as periodic hard drive analysis and backup, antivirus software, and hardware upgrades do exist, but, again, a straightforward solution to this eventuality would be frequent re-enrollment of individuals and re-generation of IrisCodes in order to refresh the coded data and guard against corruption.

4. Comparison

For pattern recognition, only objects with less inter-class variability than intra-class variability can be classified reliably. Because iris patterns are a

---


94 See John Daugman & Cathryn Downing, No Change Over Time Is Shown in Rankin et al. “Iris Recognition Failure Over Time: The Effects of Texture,” 46 PATTERN RECOGNITION 609, 609–10, (2013) (stating that encoding variations do not imply variations in the object being imaged); Hunny Mebrotra et al., Does Iris Change Over Time?, 8 PLOS ONE 1, 3 (2013) (observing that increase in false rejection rate is due to poor acquisition, presence of occlusion, noise, and blur).


96 See id. (“Stray particles can literally zap a zero to a one, or vice versa, introducing random corruption even when a computer is turned off. And if stray particles don’t do the trick, simple physical decay can. Magnetic drives lose their orientation, electrically charged media gradually lose charge, and optical media breaks down as its plastic degrades or is damaged. In a sense, then, computers are literally doomed to become increasingly corrupt as time goes on, and all digital storage will eventually be ruined.”).

97 Id.

98 Id.

99 Daugman, supra note 25, at 21.
highly robust and distinctive biometric, different images of the same iris vary little, while images from different irises vary significantly. IrisCodes can be compared for either identification (i.e., one to many), or verification (i.e., one to one). A database with millions of iris pattern records can be searched in under a second. Since no two images of a single iris produce the exact same IrisCode, iris recognition systems use a similarity score to match an IrisCode to an existing template. The threshold for determining whether an IrisCode and template are similar enough to be a match is determined by the scanner’s setting.

The dissimilarity between IrisCodes is called the “Hamming Distance” (HD). HD is defined as the number of bits that differ between two different lengths of code. Calculation of HD is a way to evaluate the closeness of the match between IrisCodes. Evaluating similarity requires setting a threshold for comparison of IrisCodes: HDs below the threshold indicate a match, and HDs above it indicate a non-match. An optimal decision threshold (an equal probability of false-accept and false-reject errors) is typically the point at which the two distributions (match versus non-match) cross over.

It is extremely improbable for two different irises to disagree in less than about a third of their bits. Because so many different iris pattern features are distinguishable, the likelihood of two different irises generating the same information is statistically impossible. Daugman's research revealed that

[For] 9.1 million iris comparisons . . . the smallest [HD] observed was 0.334. . . . [T]he probability of such an event is

---

100 See supra Section I.A (“These inherent physical aspects of iris structure directly bear on its biometric value. Scientists and analysts objectively determine biometric efficacy in terms of robustness and distinctiveness.”) (footnote omitted).
101 Daugman, supra note 25, at 23. The high confidence levels of iris recognition enable exhaustive searching of national databases without false matches, whereas other biometrics can only survive relatively few comparisons. Id. at 22.
102 Id. at 23. By dividing a database into units of about one-hundred-thousand persons each, and running independent search engines in parallel, one could search national iris pattern databases with a high level of confidence in about one second using several inexpensive central processing units (“CPUs”). Id. at 28.
103 Zetter, supra note 85.
104 Id.
105 Named for Richard Hamming, who introduced the concept that subsequently became fundamental for information and coding theory, as well as cryptography. R.W. Hamming, Error Detecting and Error Correcting Codes, 29 BELL SYST. TECHNICAL J. 147, 147–160 (1950).
106 P. DANZINGER, LINEAR CODES, 1, http://www.math.ryerson.ca/~danziger/professor/MTH108/Handouts/codes.pdf [https://perma.cc/4VYW-MS34] (last visited Dec. 21, 2016). For example, since 01101010 and 11011011 differ in four places, the Hamming distance d(01101010, 11011011) = 4. Id.
107 Wildes, supra note 9, at 1359.
108 Id.
109 Id.
110 Daugman, supra note 25, at 24.
IRIS RECOGNITION, FORENSICS, AND THE FUTURE OF PRIVACY

about 1 in 16 million. . . . Thus, even the observation of a relatively poor degree of match between the phase codes for two different iris images (say, 70% agreement or HD = 0.300) would still provide extraordinarily compelling evidence of identity, because the test of statistical independence is still failed so convincingly.¹¹¹

This failure of a test of statistical independence on phase structure encoded by the 2D Gabor wavelets is the principle behind iris recognition.¹¹² When comparing two different irises, the test of statistical independence is failed when less than one-third of the bytes in the codes differ.¹¹³ When images of the same iris are compared, they fail the test—thus, paradoxically, indicating a perfect match.¹¹⁴ Conversely, if the HD detected between different images is above the set threshold, the iris-recognition system declares the images a nonmatch.¹¹⁵ The core theory behind Daugman’s algorithms is that the failure of a test of statistical independence is a strong basis for pattern recognition if there is sufficiently high entropy (enough random variation) among samples from different classes.¹¹⁶ With a false match rate of about one in a million, this creates an acceptable and practical level of security.

5. Decision

The greatest strength of iris recognition is its astronomically low false-match probability. According to Daugman, in all of the published scientific tests of its algorithms, there has never been a single documented false match.¹¹⁷ He has stated, “[a]ll testing organizations have reported a false match rate of 0 in their tests, some of which involved millions of iris

¹¹¹ Id.
¹¹² Id. at 21. “[T]he combinatorial complexity of this phase information across different persons spans about 249 degrees of freedom and generates a discrimination entropy [information density] of about 3.2 bits/mm² over the iris, enabling real-time decisions about personal identity with extremely high confidence.” Id.
¹¹³ See id. at 26 (asserting that iris recognition is primarily based on a test of statistical independence: “Any two different irises are statistically ‘guaranteed’ to pass this test of independence[,] and any two images that fail this test [i.e. produce a HD ≤ 0.32] must be images of the same iris”).
¹¹⁴ See id. (“The fact that the minimum HD observed in all of these millions of rotated comparisons was about 0.33 illustrates the extreme improbability that the phase sequences for two different irises might disagree in fewer than a third of their bits.”).
¹¹⁵ Id.
¹¹⁶ See id. at 23 (“The key to iris recognition is the failure of a test of statistical independence, which involves so many degrees-of-freedom that this test is virtually guaranteed to be passed whenever the phase codes for two different eyes are compared, but to be uniquely failed when any eye’s phase code is compared with another version of itself.”).
¹¹⁷ See Nicholas Orlans, Eye Biometrics: Iris and Retina Scanning, in BIOMETRICS 93 (2003) (noting that iris recognition tests are “almost flawless,” and that the odds of two irises generating a false match are theoretically one in 1.2 million).
pairings.

The practical effect of this extremely low probability of a false match, given an HD ≤ 0.32, is that nation-sized databases can be exhaustively searched with a high level of confidence in the result.

Because of its high degree of accuracy, iris recognition is reliable for identification as well as verification purposes. Identification is a much more demanding process than verification, even for modest databases, thus not all biometrics that serve adequately as verifiers have equal utility for identification. Iris recognition relies on comparison of the HD distributions for the same versus different irises in order to decide if a match is statistically probable. Also, the HD threshold is adaptive, meaning it maintains the same level of certainty regardless of database size. Therefore, if the search database contains one million different iris patterns, the HD match level need only be adjusted from 0.33 to 0.27 in order to maintain a net false match probability of $10^{-6}$ for the entire database.

II. HOW CAN IRIS SCANS BE USED?

Although previously used mostly for high-level security, iris recognition’s increased economic viability and technical maturation have rendered it broadly applicable in both the public and private sectors. Iris recognition has already been used extensively, both domestically and abroad; the question now is, what other purposes might it be used for in the near future? There has been a proliferation of algorithm advances and providers since Daugman’s patent expired in 2005. And it has been

---

118 Daugman, supra note 25, at 22.
119 Id. at 28.
120 See id. at 26–27 ("The requirements of operating in one-to-many ‘identification’ mode are vastly more demanding than operating merely in one-to-one ‘verification’ mode (in which an identity must first be explicitly asserted, [and] then verified . . . by comparison against [a] single nominated template.").
121 See id. at 27 (describing how the overlap between dual distributions reveals the extent to which they are separable and determines decision error rates and reliability).
122 Id.
123 Id.
124 See, e.g., Woodward, supra note 6, at 109–11 (describing how access to sensitive areas can be secured using biometrics).
125 See, e.g., id. at 98 (noting that “the U.S. Secret Service and the General Accounting Office [have given] biometrics a qualified endorsement as a viable means to deter fraud in government entitlements distributed electronically”).
126 See, e.g., Roger J. Chin, Gregory Hennessy & Toby Madubuko, India’s Aadhaar Project: The Unprecedented and Unique Partnership for Inclusion, 12 J. ADMIN. SCI. 1, 1–2, 5 (2015) (discussing India’s Unique Identification Authority program for identification of its 1.2 billion citizens by providing each a unique 12-digit ID number, called an Aadhaar). Each person’s Aadhaar is linked to her basic demographic and biometric information, including fingerprint and iris scans, which are stored in a centralized database. Id. at 5. The program’s slogan is “To give the poor an identity.” HANDBOOK OF IRIS RECOGNITION vii (Kevin W. Bowyer & Mark J. Burge eds., 2d ed. 2016).
127 Other advancements include: increased camera availability, lower failure to capture rates, faster capture time, and decreased cost of data storage. NAT’L SCI. & TECH. COUNCIL, BIOMETRICS IN GOVERNMENT POST-9/11: ADVANCING SCIENCE, ENHANCING OPERATIONS, 79 (Aug. 2008),
observed that “[t]echnology is fast. The law . . . is slow.” To keep up, we must anticipate the direction in which biometrics generally, and iris recognition in particular, are headed.

A. Identification

Biometric identification falls under two major categories: positive and negative. Positive-identification systems test whether a submitted image belongs to an individual already enrolled in the system. This serves not only to confirm the identity of the individual, but it prevents multiple individuals from using a single identity. Conversely, negative-identification systems test whether the submitted image belongs to an individual not already enrolled in the system. This prevents an individual from having multiple identities in the system. Both positive and negative identification serve the same goal: to authenticate each individual based on a single, non-transferable identity.

Of course, not all identifications carry the same weight. For example, iris scanning has been used all over the world as a “living passport.” It has also been used in many countries for the proper allocation of government benefits. Additionally, in private commercial settings, consumers may be scanned in an effort to predict behavior based on past purchases. Sometimes, iris recognition comes in handy for atypical situations. For example, National Geographic used iris scanning to identify a famous Afghan girl with haunting eyes who had been featured on the magazine’s cover eighteen years earlier. But for iris recognition to be used in a forensic context, experts must demonstrate that it is the product of sound scientific methodology and principle.

The use of iris recognition technology is widely accepted in the


130 Id. Positive identification systems are typically used to control access to high-security areas or networks. See id. (describing how positive identification is used to regulate airport employee access).

131 Id.

132 Id.

133 Id.


scientific community as a valid method for human authentication. Like all reputable biometrics, iris scanning is based on the scientific method. Under the Frye standard, forensic evidence could be presented as long as the underlying theory was “generally accepted.” However, the codification of Article VII of the Federal Rules of Evidence in 1975, and the Supreme Court’s subsequent determination that Article VII legislatively overruled Frye, yielded a more demanding standard for experts presenting scientific evidence. Under the Daubert standard, expert testimony given regarding forensic science and biometrics is admissible when it has sufficient safeguards of reliability and relevance.

The reason behind this caution in admitting expert biometric testimony is the tendency for laymen to have unsubstantiated faith in anything deemed “scientific.” Although this Note has established that iris recognition is a reliable and accurate technique, it has also acknowledged that it is vulnerable to fraud and human error. Although not a complete indictment, we must continuously ensure that our trust in biometrics is well founded. The cost of failing to do so exceeds the benefit, considering “[t]he difficulty of challenging a false biometric reading and the potential for [resulting] improper assumptions . . . particularly . . . given the settings in which biometrics are likely to be used.”

136 Hoffman, supra note 2, at 41.
137 Id.
138 See Frye v. United States, 293 F. 1013, 1014 (D.C. Cir. 1923) (“Just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized, and while courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs.”) (emphasis added).
139 FED. R. EVID. 702–03.
141 Hoffman, supra note 2, at 42.
142 Daubert, 509 U.S. at 579.
143 Id. at 593–94 (listing empirical testing, peer review and publication, known or potential rate of error, standards and controls, and degree of general acceptance by the relevant scientific community as non-exclusive factors relevant in establishing the validity of scientific testimony).
145 See supra Section I.B.iv.
146 See supra Section I.B.v.
147 Robin Feldman, Considerations on the Emerging Implementation of Biometric Technology, 25 HASTINGS COMM. & ENT. L.J. 653, 666 (2003). The liberty of a criminal defendant, although protected somewhat by due process, is at stake. Therefore, iris recognition, or any biometric technology, must be subject to a high level of legal scrutiny.
B. Surveillance

For some, iris scanning raises the specter of government tracking, particularly because an iris image need not be voluntarily provided. The fear that government agents will be able to monitor individuals by mass collection of biometric data is not without reason. Powerful biometrics, such as iris scanning, do make identification easier, and unlike a credit card number, an iris pattern is not easily reissued. This explains why “[stealing] biometric information amounts to permanent identity theft.”148 Non-biometric tracking is already done on a large scale,149 but the greater concern is that once an individual is enrolled in a database, there are few ways to discreetly evade detection.150

The fact that iris scans can be collected without knowledge or consent presents an ideal opportunity for would-be surveillants. Since a person cannot change his or her iris pattern without risking blindness,151 the potential exists for iris recognition to substantially facilitate tracking beyond the capacity of even other biometrics. This is due in large part to the “nearly instantaneous data sharing” that current biometric technological and communication advances allow.152 This explains why “biometrics have become increasingly instrumental in enforcing criminal and immigration law, detecting persons known to pose a threat to public safety and national security, and preventing fraud.”153

As the paragon of all law enforcement and intelligence organizations, the Federal Bureau of Investigation has long had an interest in biometrics. But following the 9/11 attacks, that interest grew into a national obsession. To help “increase the range and quality” of its “biometric identification capabilities” the FBI launched three biometric initiatives: Next Generation Identification (NGI), Combined DNA Index System (CODIS), and the Biometric Center of Excellence (BCOE).154 Government funding for biometrics research has also proliferated after 9/11.155 Some of these funds

---

150 Supra note 67, at 2 (noting that eyeglasses, contact lenses, and sunglasses do not obscure an individual’s iris pattern).
151 Daugman, Visual Recognition, supra note 14, at 1148.
153 Id.
155 See BIOMETRICS POST-9/11, supra note 127, at 17–18 (“[A]lthough the U.S. government funded iris recognition research for several years prior to 9/11 . . . [t]o improve the utility, performance, and
took the form of federal sponsorship of academic programs to foster rapid development of iris biometric technology. The result is a swiftly evolving state of art and interoperability.

Iris recognition and other biometrics become even more powerful when the database becomes larger and is shared among several governmental agencies—the more people enrolled in a system and the more people that have access to that system, the fewer places there are left to hide. At a certain point, mere non-enrollment of an individual may be sufficient cause for suspicion and subsequent investigation.

C. Security

Iris recognition has readily apparent applications for maintaining security interests. The FBI's Criminal Justice Information Services (CJIS) Division developed and integrated NGI to replace the Integrated Automated Fingerprint Identification System (IAFIS). The FBI describes NGI as "the world's largest and most efficient electronic repository of biometric and criminal history information." Indeed, the quantity and breadth of identifying information in the NGI system is unprecedented. The FBI describes its NGI system as "a platform for multimodal functionality that will continue to evolve with new technologies and user requirements."

The impetus behind pushing these boundaries is nebulously framed as a response to "growing threats.

Prior to 9/11, the U.S. government had already begun to develop automated, multimodal systems for identifying people at a distance for ease-of-use... [it] substantially increased its investment after 9/11."). Advancements such as increased standoff distances, improved system performance (through reduced size and cost), and enhanced moving image acquisition capability were the result of such increased funding. Id. Some of these developments include: analysts' tools to augment automated iris match algorithms, and multiple matching algorithms, including government-owned algorithms. Id. See Next Generation Identification (NGI), FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi [https://perma.cc/7H57-ZJQ6] (last visited Oct. 30, 2016) (describing how the implementation of NGI increased the completeness, efficiency, and accuracy of biometric identification services previously accessible through IAFIS).

protection and early warning. One such program, the Defense Advanced Research Projects Agency (DARPA)’s Human Identification at a Distance (HumanID) program, which began in September of 2000, provided the scientific foundation for human identification at a distance, including iris recognition. After 9/11, the Department of Defense (DoD) expanded the role of the Biometrics Management Office (BMO) and Biometrics Fusion Center (BFC) beyond evaluating biometrics as a way to secure American facilities and networks.

In 2004, the DoD deployed its Automated Biometric Identification System (ABIS), a database compatible with IAFIS, to provide centralized storage for military-collected biometric data. In 2005, the Department of Homeland Security (DHS) and the Intelligence Technology Innovation Center (ITIC) co-sponsored a study of iris recognition accuracy, utility, and interoperability, known as Independent Testing of Iris Recognition Technology (ITIRT). Also, from 2005 to 2006, the National Institute of Standards and Technology (NIST) conducted the Iris Challenge Evaluation (ICE), a two-phase “large-scale, open independent technology evaluation for iris recognition . . . to promote [its] development and . . . assess its state-of-the-art capability.” In September of 2013, the FBI deployed an iris recognition pilot program to evaluate existing technology, address challenges, and develop a capable system.

The creation of a comprehensive database is a logical precursor to maximizing the utility of iris biometrics. Although the FBI claims that ABIS and other biometric platforms are necessary tools in identifying known or suspected terrorists, it remains unclear whether widespread deployment

---

162 See BIOMETRICS POST-9/11, supra note 127, at 18 (stating that the initial maximum distance for recognition of cooperative subjects, under controlled illumination was less than ten feet, but by the program’s end in 2003, that distance had increased to 150 feet).

163 See id. ("[T]he HumanID program made significant gains in understanding the difficulties associated with biometric technology and provided the ground work for numerous future biometric research programs.").

164 Id. at 25.

165 Id.


168 See supra note 158 (asserting that the iris recognition pilot program provides CJIS the means for continual assessment and development of privacy policy, image capture best practices, camera requirements, image compression specifications, and image quality metrics).

169 See BIOMETRICS POST-9/11, supra note 127, at 25. Various examples of interagency database cooperation cited include discovery of insurgents applying for selection to the Iraqi Police Academy, and matching foreign detainees to U.S. felony records. Id.
of this technology has correspondingly improved public safety. National security is a largely convincing justification for mass data-collection, retention, and sharing. But the strategy for gathering such information, as well as the duration of its storage, should be clearly defined and narrowly tailored to achieving that end. Similarly, measures to restrict the transfer of biometric information among government agencies should be implemented to limit incursions on privacy.

There appears to be a growing host of entities interested in and motivated to share biometric information. Although government agencies constitute a major portion of that group, industry and academia have also made major contributions to the research, development, testing and evaluation of iris recognition technology. The use of a common infrastructure, coupled with NGI’s integration and indexing of multimodal biometric data, continues to expand the practical limits of iris recognition technology.

III. IRIS RECOGNITION AND THE LAW

It remains to be seen whether iris recognition will be determined to constitute a “search” within the meaning of the Fourth Amendment, despite the fact that it does not entail a bodily intrusion. Iris scanning involves controversial legal issues implicating constitutional safeguards as well as larger public-policy concerns. Given the pervasive integration of biometric scanning into government programs, these legal and policy concerns must be addressed. To fill the regulatory gap, we first need to define iris recognition in legal terms, and then decide whether its benefits

---

170 See id. at 13 ("All federal biometrics RDT&E is closely prioritized and coordinated through the [National Science and Technology Council] Subcommittee on Biometrics and Identity Management and often involves joint sponsorship and project management from multiple agencies.").

172 Biometrics, DEPT. HOMELAND SEC., https://www.dhs.gov/biometrics [https://perma.cc/7BDZ-LZP9] (last visited April 20, 2017) (listing the Department of Homeland Security, Department of Defense, Department of Justice, and Department of State as government agencies that collect and share biometric information); Robyn Caplan et al., Biometric Technologies in Policing, DATA & CIVIL RIGHTS: A NEW ERA OF POLICING AND JUSTICE 1, 3 (Oct. 27, 2015) http://www.datacivilrights.org/pubs/2015-1027/Biometrics_Primer.pdf [https://perma.cc/PVS3-2WMK] ("Collection of biometric data is not restricted to any one government agency, and is occurring at the local and state level, as well as through federal agencies such as the . . . FBI, DEA, NSA, TSA and others. . . . Data is also increasingly being shared between these different levels of government, and between agencies.").

172 BIOMETRICS POST-9/11, supra note 127, at 79; see also West Virginia University Named National Leader for FBI Biometrics Research: WVU-FBI Partner on Biometric Center of Excellence, FBI (Feb. 6, 2008), https://archives.fbi.gov/archives/news/pressrel/press-releases/west-virginia-university-named-national-leader-for-fbi-biometrics-research [https://perma.cc/ME7L-BECC] ("WVU’s role is to provide biometrics research support to the FBI and its law enforcement and national security partners and serve as the FBI liaison to the academic community of biometric researchers nationwide.").

173 Woodward, supra note 6, at 99, 115, 117, 121.
outweigh its costs. Only then can we choose to enforce those situations iris recognition can be used, and those when it should be excluded.

A. Privacy

In their classic law review article The Right to Privacy, Samuel Warren and Louis Brandeis popularized Judge Thomas M. Cooley’s phrase articulating privacy as “the right to be let alone.”174 The text of the Constitution does not define privacy, and the legal community has struggled to adequately explain it. The term’s lack of clarity is complicated by the fact that it is a social construct,175 and our perception of privacy is constantly evolving. Still, perhaps the most enduring thread in the concept of privacy is the notion of control. Iris recognition technology and other biometrics have the potential to allocate vast control to their users and to greatly undermine that of the subjects. As a threshold matter, we must resolve whether iris recognition is compatible with maintaining privacy.

The Supreme Court has implicitly recognized three distinct forms of privacy: physical, decisional, and informational.176 Physical privacy is typically understood to be “freedom from contact with other people or monitoring agents.”177 Decisional privacy has been defined as freedom to make private choices about personal and intimate matters without undue government interference.178 Informational privacy involves the freedom to limit others’ access to certain personal information.179 The “personal decisions relating to marriage, procreation, contraception, family relationships, child rearing, and education,”180 relating to decisional privacy are not clearly implicated by iris scanning technology. We will consider, in turn, the effect of iris recognition technology on physical and informational privacy.

1. Physical Privacy & the Fourth Amendment

Although some iris scanning may involve voluntary enrollment for convenience or other purposes, government-mandated biometrics threaten to violate physical privacy. The Fourth Amendment, which governs searches and seizures conducted by government agents, provides physical privacy in that “[t]he right of the people to be secure in their persons, houses, papers,

---

174 Id. at 120.
175 Id. at 117–21; see also RICHARD C. TURKINGTON ET AL., PRIVACY: CASES AND MATERIALS 35 (1992) (“Law mirrors the society that creates it.”).
176 Woodward, supra note 6, at 122.
177 Id.; see also Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (describing physical privacy).
178 Woodward, supra note 6, at 122.
179 Id.
and effects, against unreasonable searches and seizures, shall not be
violated." By its very nature, iris scanning qualifies as a search in terms of
the Fourth Amendment.

Courts have looked to three situational aspects in determining a search’s
constitutionality: The nature of the intrusion, the scope of intrusiveness, and
"reasonableness." Blood-drawing, DNA collection, breathalyzer tests,
and urinalysis have all been held to constitute Fourth Amendment
searches. Also, a search need not involve an actual penetration of the
body. Despite the fact that no reasonable expectation of privacy exists in
facial characteristics "constantly exposed to the public," the process of
storing, retrieving, and analyzing an IrisCode can independently qualify as
a search because of the depth of inspection it allows.

Facial and iris recognition differ for the purpose of Fourth Amendment
searches because of the operative gulf between facial- and iris-recognition
technologies, which creates disparate privacy consequences. Facial
recognition remains a central problem in computer vision because the
existing technology cannot infer from images what humans can: the 3D
arrangement of objects from their mutual occlusions; object surface

181 U.S. CONST. amend. IV.
individual must have an actual expectation of privacy (subjective test) and that expectation must be
reasonable under the circumstances (objective test)); but see Christopher R. Jones, Note, "EyePhones":
A Fourth Amendment Inquiry into Mobile Iris Scanning, 63 S.C. L. Rev. 925, 947 (concluding that, in
the context of police officers’ use of mobile iris-scanning technology, a search would not occur under
current Supreme Court jurisprudence).
183 Woodward, supra note 6, at 124; see also Vernonia Sch. Dist. 471 v. Acton, 515 U.S. 646, 654,
658, 660 (1995) (considering factors including: the nature of the privacy interest, the character of the
intrusion, the information the intrusion discloses, and the nature and immediacy of the governmental
concern, in determining a search’s constitutionality).
that a ‘compelled intrusion[n] into the body for blood to be analyzed for alcohol content’ must be deemed
a Fourth Amendment search. . . . Subjecting a person to a breathalyzer test, which generally requires the
production of alveolar or ‘deep lung’ breath for chemical analysis, implicates similar concerns about
bodily integrity and, like the blood-alcohol test . . . should also be deemed a search. . . . [I]t is clear that
the collection and testing of urine intrudes upon expectations of privacy that society has long recognized
as reasonable, the Federal Courts of Appeals have concluded unanimously, and we agree, that these
intrusions must be deemed searches under the Fourth Amendment.") (internal citation omitted); Schmerber v. California, 384 U.S. 757, 767–68 (1966) (stating the Fourth Amendment’s proper function
is to constrain against intrusions into the body which are not justified); United States v. Mitchell, 652
F.3d 387, 406 (3d Cir. 2011) (emphasizing DNA collections are subject to the strictures of the Fourth
Amendment).
185 See Skinner, 489 U.S. at 616 ("[i]t is obvious that this physical intrusion, penetrating beneath
the skin, infringes an expectation of privacy . . . [but] [t]he ensuing chemical analysis of the sample to
obtain physiological data is a further invasion of . . . privacy interests. . . . Nor can it be disputed that the
process of collecting the sample to be tested . . . itself implicates privacy interests.").
187 See Cupp v. Murphy, 412 U.S. 291, 295 (1973) (arguing that the scraping of dried blood from
underneath fingernails is a search because it allowed closer laboratory examination than normal public
view).
properties, such as texture and color; depth and volumetric object properties from their 2D images; structure from motion, shading, texture, shadows, 3D shape from a 2D line drawing; recognizing a 3D object regardless of its rotation in 3D space; and understanding a novel object. These difficulties are apart from the separate problem that faces (unlike irises) change significantly with age, expression, makeup, speaking, and so on. Compared to iris recognition, facial recognition technology is abysmally inaccurate and unreliable. For example, a computer cannot match a front and side view of the same face (a task which a person could perform easily), whereas a computer can match an iris image to the correct IrisCode from amongst millions of templates.

Both the face and the eyes upon it are normally publicly exposed. But because iris recognition technology allows for acquisition, storage, retrieval, and analysis of personally identifying data, an iris scan independently qualifies as a search where a facial scan does not. Additionally, public facial exposure is a social norm in most cultures, its acceptance probably due to the face’s function as an expressive and communicative organ. But despite the Supreme Court’s decision in Dionisio that there is no expectation of privacy in facial features exposed in public—the eyes and iris are a part—there is actually more privacy inherent to facial features than iris pattern.

Due to the constraints of automated facial recognition discussed above, there are limits to the information generated by public exposure of one’s face. Facial recognition performed by humans is a function of audience familiarity with the subject’s face. Conversely, a single inadvertent exposure of one’s irises to scanners is sufficient to extinguish anonymity. Because iris-recognition technology is familiarity independent (once identified=always identifiable), has nearly infallible recall, has potentially broad resources, and examines subjects in far greater detail than the human eye or other biometrics, it threatens physical privacy in a way that facial recognition does not. Since public awareness of iris recognition is limited, an average person would not reasonably expect (either subjectively or objectively) to be identifiable amongst a crowd of strangers. Thus iris

---

188 DAUGMAN, supra note 46, at 5–7.
189 See id. at 4 (discussing a computer’s issues with facial recognition).
190 Supra Section I.B.1.
193 Id. at 14.
recognition, despite requiring no bodily contact and involving publicly
exposed features, can reasonably be construed to be a search within the
meaning of the Fourth Amendment.

To ascertain reasonableness, courts must balance the "intrusion on the
individual's Fourth Amendment interests against its promotion of legitimate
governmental interests."194 Also, a search is deemed "reasonable' only if
the police have probable cause or reasonable suspicion of criminal
activity."195 But a search warrant may not even come into play. Valid
government interests such as counter-terrorism, border control, and proper
allocation of government-funded benefits could theoretically provide law
enforcement the ideal pretext for dragnet scanning of virtually the entire
population. This scenario would undermine the Fourth Amendment's core
animating purpose and endanger other civil rights that depend on the liberty
despite privacy that it ensures.196

2. Informational Privacy

The right to informational privacy can be understood as "the claim of
individuals . . . to determine for themselves when, how, and to what extent
information about them is communicated to others."197 Unrestricted use of
iris recognition to indiscriminately collect, indefinitely store, and widely
disseminate citizens' information in large, centralized databases violates the
autonomy guaranteed by the Fourteenth Amendment.198 Other constitutional
protections threatened include the Fifth Amendment right against forced
revelation of private information and the implicit First Amendment right
against disclosure of private associations.199 Although the Supreme Court in
1965 formally acknowledged a constitutional right to privacy drawn from

194 Woodward, supra note 6, at 124.
195 Id.; see also Casey A. Taylor, The Fiction of Privacy Under the Fourth Amendment: Examining
(asserting that the government bears the burden of showing the permissibility of a warrantless search, if
a search was found to be conducted in an area one expects, by reasonable societal standards, to be
private).
196 See, e.g., Monrad G. Paulsen, The Exclusionary Rule and Misconduct by Police, 52 J. CRIM. L.
CRIMINOLOGY & POLICE SCI. 255, 264 (1961) (stating that all other freedoms depend on the preexistence
of security and privacy).
197 Alan F. Westin, PRIVACY AND FREEDOM 7 (1967); see also ROBERT ELLIS SMITH, BEN
FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE
INTERNET 6 (2000)
("[Privacy] is the desire by each of us for physical space where we can be free of interruption, intrusion,
embarrassment, or accountability and the attempt to control the time and manner of disclosures of
personal information about ourselves. In the first half of our history, Americans seemed to pursue the
first, physical privacy; in the second half—after the Civil War—Americans seemed in pursuit of the
second, 'information privacy.'").
198 U.S. CONST. amend. XIV.
199 Id. amend. V; id. amend. I.
the “zones” of freedom created by these individual rights, it has chosen to defer to the legislature despite its concern that emerging biometric technologies, like iris recognition, might erode informational privacy.

Informational privacy concerns the use of information pertaining to an individual, particularly “the extent of the individual’s authority to control how that information is used . . . and the corresponding responsibility of other individuals and organizations to include the individual in decision-making processes that drive subsequent use.” The impetus behind the emergence of informational privacy (as distinct from physical privacy) was the simultaneous advent of new technology and increasing demand for personal information. These two events merged to form the backdrop against which Warren and Brandeis asserted an individual right to prevent unintended publication of personal information.

Personal information is defined as “any information that could be used to identify an individual.” Biometric information, such as IrisCodes, is personal information due to both content (collected from observation of individuals) and use (general purpose of biometrics is recognition of individuals). Thus, when biometrics are collected, personal information is always involved and privacy interests are necessarily triggered. Regardless of the intent behind collection, ongoing privacy assessments should be conducted to analyze the potential impact of iris scans on individual privacy interests. A comprehensive privacy assessment would begin with direct use of information gained from iris scans (i.e., iris image, IrisCode) and continue with a thorough investigation of all subsequent uses of that data for

---

200 See Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (“Specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance . . . [v]arious guarantees create zones of privacy.”)

201 See Whalen v. Roe, 429 U.S. 589, 605 (1977) (“We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.”).


203 Id. at 28 (“Earlier cameras were large and slow and required the intentional participation of the subject. The new cameras were smaller and faster and made it easy for one individual to photograph another without permission or even awareness. At the same time, ‘gossip’ newspapers erupted in popularity creating a vacuum for content about individual personal lives.”). Both the emergence of new technology, such as iris recognition, and increasing demand for personal information translate readily to modern times.

204 Id.

205 Id. at 34.

206 See id. at 35 (defining biometric information).

207 Privacy entails the freedom to make personal decisions without unwarranted government interference. See Indus. Found. of the S. v. Tex. Indus. Accident Bd., 540 S.W.2d 668, 679 (Tex. 1976) (“It is also apparent that the right of privacy is primarily a restraint upon unwarranted governmental interference or intrusion into those areas deemed to be within the protected ‘zones of privacy.’”).
Individuals may choose to forfeit their informational privacy by informed consent to iris scanning. But if individuals do not voluntarily submit to iris scanning, they should not be deprived of other rights in exercising their right to informational privacy. To ensure the protection of privacy interests, an organization administering an iris recognition system or making decisions based on data collected should be subject to external auditing. Absent specific common-law requirements for informed consent to iris scanning, it falls to the legislature to enact a statute or direct regulation. The following subsection of this Note will focus on suggested guidelines for the contours of such legislation.

B. The Future

As a matter of public policy, legislation that regulates the use of iris recognition technology should be clearly articulated, disclosed in advance, and narrowly tailored to the original purpose. Legally founded deployment of iris scanning should specifically circumscribe appropriate contexts, extent of use, and access to collected information. Further, the authority collecting, using, or sharing the data must continually demonstrate a legitimate need for such information, and that the data is both within the scope and in significant furtherance of the original purpose.

In theory, this seems fairly straightforward, but in practice, iris recognition presents several challenges. First, tracking of individuals by government or other entities under the penumbra of “security” would be difficult for an average citizen to detect, let alone challenge.209 Conspicuous compliance measures, such as statutorily mandated signage and documentation of notice, would likely improve transparency. Second, iris-recognition systems may exist in multiple jurisdictions (federal, state, local), and may even cross international boundaries.210 Effective legislation would therefore require harmonization with each jurisdiction’s relevant laws. For example, the Universal Declaration of Human Rights adopted by the United Nations (and implicitly, by its member states) recognizes: “No one shall be subjected to arbitrary interference with his privacy . . . . Everyone has the

208 See PRIVACY & BIOMETRICS, supra note 202, at 35 (arguing a privacy assessment “should start with direct use of biometric information and expand to cover all uses of data that become part of an identification and decision-making process.”).

209 See, e.g., Iris Scanners Can Now Identify Us From 40 Feet Away, CONVERSATION (May 21, 2015), https://theconversation.com/iris-scanners-can-now-identify-us-from-40-feet-away-42141 [https://perma.cc/4GED-BGE6] (noting that researchers were able to obtain driver’s iris scans from the reflection in their vehicle’s side mirror).

210 Jurisdictional overlap may occur through a system’s physical equipment, the information it contains, the individuals using or benefiting from it, and/or the individuals related to information that it uses. PRIVACY & BIOMETRICS, supra note 202, at 32–33.
right to the protection of the law against such interference . . . "

Third, there are small but tangible gaps in accuracy and reliability at various levels of iris-recognition technology, including biographic information linking, image-to-template conversion, and matching statistics. Because a possibility exists that a probable match is not an actual match, legislation must allow for individuals to dispute matching decisions, and request erasure of incorrect data.

There are also many considerations in determining iris recognition's applicability: environment, security and throughput needs, desired task (identification versus verification), associated costs, interoperability, and user acceptance. Despite these challenges, iris recognition technology must be addressed in order to achieve valid objectives without eradicating privacy interests. Iris-recognition systems are rapidly growing in use around the world by law enforcement agencies and the commercial sector, creating the potential for a "digitally efficient investigative state." Existing legislation such as the Freedom of Information Act, the Privacy Act of 1974, and the E-Government Act of 2002 can help provide a foundation in determining the necessary architecture to ensure individual privacy protection.

CONCLUSION

Iris recognition technology is being implemented right now in a growing number of industrial and governmental settings. This biometric has already begun to cause high-order disruptive change to social perception of privacy, which will likely continue. The first step in enabling coexistence of iris recognition technology and personal privacy is deciding what we want our collective future to look like. There will always be a tension between security and privacy—the challenge remains to find a balance and accept the sacrifice required to maintain it. Iris recognition should be thoughtfully and minimally deployed in order to mutually protect privacy and promote security to the greatest extent practicable.

212 PRIVACY & BIOMETRICS, supra note 202, at 7–9.
213 Daugman, supra note 25, at 27.
216 SRI INT’L, supra note 67, at 2 ("Amsterdam’s Schiphol and other airports use iris recognition to provide self-service passport control; law enforcement agencies across the U.S. use it to identify people; hospitals and mandatory drug testing labs use it to ensure patient identity; countries such as India are implementing nationwide iris identification initiatives; enterprises such as Google use iris recognition to control physical access.")