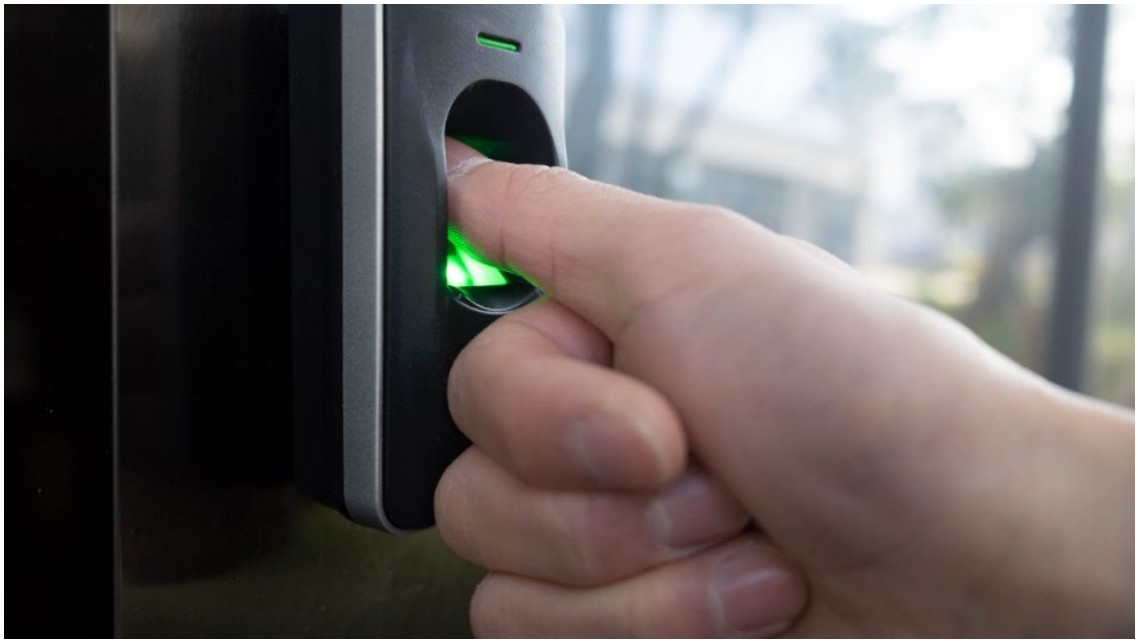
January 01, 2024 DEPARTMENTS

Technology—Probate - The Intersection of Biometric Information and Estate Planning

Editor: Ross E. Bruch, Brown Brothers Harriman & Co., One Logan Square,14th Floor, Philadelphia PA 19103. Contributing Author: Justin Brown, Ballard Spahr, 1735 Market Street, 51st Floor, Philadelphia, PA 19103.

Share:



> "Biometric information" is any information, regardless of how it is captured.
> *(Source: Getty Images)*

Technology—Probate provides information on current technology and microcomputer software of interest in the probate area. The editors of Probate & Property welcome information and suggestions from readers.

Biometric information has become widely used and accepted in many aspects of our lives. Using biometric information is convenient and purportedly secure, so individuals will often willingly turn over their unique biometric information

without considering the potential consequences of data breaches. Facial scans and fingerprints have become the primary method to unlock phones, tablets, computers, and apps. Wearables record our heart rates every second of the day to determine our steps, activity, and general overall health, and in the process, amass and transmit massive amounts of medical data to third parties.

Apple's latest software updates in iOS 17 introduced the use of Personal Voice, an accessibility program designed to afford those who may lose the ability to speak in the future a way to talk again through their AI-generated voice. After only fifteen minutes of a user reading 150 text prompts, the software records the user's voice and creates a mechanism to mimic the user's voice. Simply type in a phrase, and Personal Voice will recite the phrase in the user's voice. Although Personal Voice is not yet a spot-on replica of a user's voice, the potential for mimicking a user's AI-generated voice is just around the corner.

Amazon recently announced its plans to allow Whole Foods customers to pay at all their stores by the year's end by simply waving their hands. A customer's palm print will be linked to the customer's credit card so that customers will no longer need their wallets or phones to pay for groceries.

Apple's Vision Pro will soon enable users wearing the device during a FaceTime call to reflect a digital representation of themselves, called a Persona, based on their biometrics and Apple's machine learning. The person on the other side of a FaceTime call will not actually see the person—instead, they will see the person's digital Persona, which is expected to look identical to the person.

"Biometric information" is any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifiers used to identify an individual. A "biometric identifier" is a unique biological trait that may identify an individual, such as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

Integrating biometrics into our lives is more convenient and secure than alphanumeric passwords. Alphanumeric passwords are often forgotten and easily hacked, and individuals, contrary to the advice of cyber security experts,

recycle their passwords, thereby making their digital lives more vulnerable to cyber-attacks. Using biometrics purports to solve this problem because instead of using vulnerable passwords, we can now use our unique biometric identifiers, which are more difficult to hack and impossible to forget, as the secure gatekeepers to our digital lives. But unlike alphanumeric passwords, social security numbers, or phone numbers, biometric information cannot be changed if stolen or compromised. Once biometric data is stolen or compromised, the individual is forever compromised. You can't exactly change your face if your facial biometric identifiers are stolen and floating around the dark web.

Because of the uniqueness of biometric information, the commoditization of biometric information has unsurprisingly expanded in the past few years. For example, facial recognition software can map out an individual's facial biometric identifiers and create a database of biometric information to be sold to law enforcement so that law enforcement may better identify individuals in crowds. Technology exists to scour pictures of individuals online and scrub their facial biometric information so that it may be collected and commoditized. This technology could be a valuable tool for law enforcement, but imagine the problems that could arise when biometric information is collected and used without an individual's knowledge for nefarious purposes. Consider the potential problems when the law enforcement biometrics database is hacked and all biometric information is in the public domain. Or consider a parent's online posting of a picture of a minor child whose biometric identifiers are scrubbed and forever in the public domain.

Some states have enacted laws to safeguard biometric information and biometric identifiers. Illinois, one of the leaders in biometric privacy, enacted the Illinois Biometric Information Privacy Act (BIPA) in 2008 and has specifically created a private right of action when an individual's biometric information is improperly collected, captured, or purchased or if such information is improperly disclosed, redisclosed, or disseminated. Earlier this year, the Illinois Supreme Court held that every improper collection, capture, purchase, disclosure, redisclosure, or dissemination of an individual's biometric information is an actionable BIPA violation, potentially subjecting

BIPA violators to significant damages. BIPA is very protective of biometric data in Illinois, but not all states have biometric privacy laws, not all states have biometric privacy laws as strict as BIPA, and no federal biometric privacy law exists at the time of this writing.

With the rise of biometrics, estate planners need to be increasingly aware of biometric information in our everyday lives because the issues surrounding biometrics affect everyone, including our clients and ourselves. Suppose biometric information is digitally stored during a client's lifetime. In that case, the client should know who is storing the biometric information, what security protocols are used to safeguard the client's biometric data from a security breach, what the storing party may or may not do with the stored information, and what happens to the biometric information if the storing party goes out of business. Clients should be cautious in turning over their biometric information out of convenience without considering the consequences of inadequate and improper storage.

For attorneys who serve as trustees of their clients' trusts that may hold cryptocurrency, many cryptocurrency custodians use biometrics for their security protocols and require verification of the trustee's biometric information to engage in a transaction. Attorneys must, therefore, ask the same questions as their clients when their biometric information is used because it is equally subject to the risks and consequences of faulty storage or a data breach.

Digitally stored biometric information appears to fall within the definition of a "digital asset" under the Revised Uniform Fiduciary Access to Digital Asset Act. Estate planners should, therefore, be considering whether biometric information may be transferred during a client's life or at a client's death, who may access the biometric information, and the proper mechanism for transferring biometric information. The data files behind Apple's Personal Voice, for example, may be stored and transferred so that a decedent's voice may be used during life or after death. Estate planners should be conversing with their clients about who should and could have access to digitally stored biometric information during life or after death, how their biometric

information may be safeguarded, and whether their biometric information should be destroyed after death to avoid misusing their biometric information. Estates of celebrities could even potentially use a celebrity's biometric information post-mortem to add value to the celebrity's estate.

Apple's Persona also creates interesting estate planning issues concerning the execution of electronic estate planning documents. Some jurisdictions permit the electronic execution of a will through Facetime with witnesses. But if witnesses see the Persona of the testator rather than the actual testator, are the witnesses actually witnessing the testator sign his will? As the use of AI with biometrics improves, there will be real questions as to whether what we see on video is "real" or if it is an AI-generated video or image extrapolated from biometric information.

In an era of digital evolution, the rise of biometric technology brings forth a dual-edged sword of immense convenience and uncharted risks. Although it promises a world where forgetting passwords becomes a tale of yesteryears and individual authentication reaches unparalleled precision, it raises profound questions about the sanctity of our most personal information. The irrevocable nature of biometric data, once stolen or misused, underscores the urgency for robust security measures and comprehensive legislative safeguards. Estate planners, now at the nexus of these technological shifts, have an imperative to adapt and provide informed guidance to their clients. As we navigate this new frontier of biometrics, balancing innovation with the intrinsic value of personal data security becomes paramount. The decisions made today will indubitably set a precedent for the future trajectory of biometric integration, demanding both vigilance and foresight.

ENTITY:

REAL PROPERTY, TRUST AND ESTATE LAW SECTION

TOPIC:

TRUSTS AND ESTATES

The material in all ABA publications is copyrighted and may be reprinted by permission only. Request reprint permission here.

Authors

Justin Brown

Technology—Probate Editor: Ross E. Bruch, Brown Brothers Harriman & Co., One Logan Square,14th Floor, Philadelphia PA 19103, ross.bruch@bbh.com. Contributing Author: Justin Brown, Ballard Spahr, 1735 Market Street, 51st Floor, Philadelphia, PA 19103.