PRIVACY AND COMPLIANCE PRISM REPORT

2025

CRASH COURSE:

THE EVOLUTION OF MODERN IDENTITY PRIVACY

A new paradigm for the emerging digital identity ecosystem.

the-prism-project.com

THE PRISM PROJECT

ACUITY MARKET INTELLIGENCE

Thank You to Our Sponsors and Partners

The Privacy and Compliance Prism Report is made possible thanks to the participation of our sponsors and partners. The biometric digital identity ecosystem depends on collaboration, and we are grateful to work with the following organizations.

SPONSORS

Anonybit

Daon

OVD KINEGRAM a KURZ company

Mitek

kantara INITIATIVE

fido ALLIANCE

European Association for Biometrics eab Human Identity in Europe

SECURE TECHNOLOGY ALLIANCE

AWARE

alcatraz

iddataweb

iiDENTIFii

KEYLESS

ZEROBIOMETRICS

PARAVISION

Corsound AI Voice Intelligence Technologies

ideem

IDEMIA PUBLIC SECURITY

DUCK DUCK GOOSE

AUTHENTIC ID

ID R&D a Mitek company

wicket

PANINI

iProov

PARTNERS

IDENTITYWEEK GLOBAL • TRUSTED • VISIONARY

ID TECH

KYC AML GUIDE

PEAK iDV

The Prism is proudly independent. While participants benefit from increased visibility and vendor profiles in this report, sponsorship does not affect a vendor's evaluation of placement within any aspect of the Prism Project.

Crash Course: The Evolution of Modern Identity Privacy

To understand how privacy and compliance are integrally linked to **digital identity transactions** and the users initiating them, it's essential to have a basic understanding of how **biometrics** entered the mainstream and impacted the evolution of **personally identifiable information (PII).** It's a fascinating portrait of a rapidly evolving technology whose adoption far outpaced corresponding policy and regulation, and how consumer education and end-user perception can both fuel technological misconceptions and inform emerging frameworks. From a consumer mass adoption standpoint, the story begins in 2013, when biometrics became a consumer product, laying the foundation for biological human identity to become a critical component of digital transactions.

This crash course is designed to familiarize the uninitiated with key digital identity definitions and concepts, contextualize them within the past decade of widespread digital transformation, and demonstrate how concepts of privacy have evolved in tandem with regulatory developments.

The Basic Idea Behind Biometrics and Digital Identity

In digital spaces, we don't have bodies, so our interactions are enabled or limited based on the **identity elements** we provide at the time of a transaction to prove we are who we claim to be. This same essential dynamic is at play during in-person transactions facilitated by digital technology. There are three types of identity elements we can provide to corroborate our identity claim: something we know **(knowledge-based authentication (KBA))** or personal identifiable information (PII), something we have token or **device-based authentication (DBA)**, a key, or a physical ID), and something we are (biometrics).

Knowledge-based authentication is the most commonly used authentication factor, but it can be guessed, shared, stolen, forgotten, or cracked. Token or device-based authentication is analogous to a traditional physical key. These factors can't be cracked or guessed, but they may be shared, lost, damaged, or stolen. Biometrics, however, stand apart as a stronger level of

Key Definitions:

DIGITAL IDENTITY TRANSACTION: An interaction, either online or in a physical space, that requires specific permissions related to an individual's identity. The scope of these transactions is broad-reaching and includes accessing email, making online purchases, verifying your age in person or online, and accessing secure physical spaces.

BIOMETRICS: Technology that uses some kind of sensor (camera, microphone, fingerprint reader, etc.) to measure or capture an image of a user's unique biological trait—most commonly a face, voice, fingerprint, or iris—and represent it via an algorithm as a **biometric template** for the purposes of identification, authentication, or security.

BIOMETRIC TEMPLATE: An algorithmic representation of a captured biological trait, stored as a mathematical value that cannot be reverse engineered to recreate a representation of the original biological trait.

PERSONALLY IDENTIFIABLE INFORMATION (PII): Data that describes foundational, biographical, and contextual details about an individual—from date and place of birth, to social security number, to address history, and more. PII linked to biometrics creates the foundation for digital identity.

IDENTITY ELEMENT: A component part of identity. In this report, an identity element refers to a biometric, a document, or metadata. An identity element can be authentic or counterfeit.

KNOWLEDGE-BASED AUTHENTICATION (KBA): A form of identity security based on knowable information. Common examples are passwords, PINs, and SMS codes.

TOKEN OR DEVICE-BASED AUTHENTICATION (DBA): A form of identity security that depends on physical possession. Common examples are keys, key cards, FOBs, USB security keys, cryptographic keys, virtual tokens, and mobile devices like smartphones when used for authentication.

assurance.

Biometrics have long represented the pinnacle of identity elements because your actual face, fingerprint, or voice cannot be shared, stolen, lost, forgotten, or easily guessed. This is a game-changing development in the rapidly converging world of digital identity transactions, spanning both physical and online spaces.

By incorporating biological identity elements into the non-corporeal interactions of online life, digital transactions approach the levels of trust we enjoy in the physical world. Things that used to require in-person interactions and painstaking identity checks, like opening a bank account or renewing a driver's license, can be performed remotely when the **relying party** (a bank or DMV in this case) can trust that a user whose biometrics match the ones associated with their digital identity is authentically themselves. This is in contrast to a person with a password or a hardware token, who can only prove they know something secret or possess something special, rather than proving they are a specific, unique human. In short, biometrics give you a body in digital spaces.

Meanwhile, physical interactions benefit from a similar boost in assurance and convenience. Unmonitored in-person transactions, such as entering a controlled workspace or a high-security restricted area, can also be secured when an individual's biometrics are verified in real-time. Whether the biometric is matched against a centralized server, locally on a door-mounted access control device, or on a personal device presented to a reader for verification, biometrics prove that the right individual at the right time with the right permission is granted physical access to restricted spaces.

To see how biometrics make this possible, and the ways in which it impacts privacy, it's essential to understand the three phases of the biometrics lifecycle:

- Enrollment: A new user submits their biometrics for the first time, creating a biometric template that will be used as the comparison for future authentication transactions. Enrollment can be strengthened with the addition of other identity elements, such as data from government-issued IDs, in a process known as i**dentity verification (IDV)**.
- Authentication: An enrolled user submits their biometrics for the purposes of matching with a template. The user's biometrics are compared to the template, and a positive match results in an authenticated transaction.

RELYING PARTY: An organization that drives end-user adoption by leveraging identity technology to improve and automate security, operations, and/or customer experience.

IDENTITY VERIFICATION (IDV): A class of identity technology that compares a user's face biometrics to the image on an identity card or credential (usually government-issued) and/or a database that stores the content of the government-issued credential, to prove a user is who they claim to be. This enables **biometric binding** as well as compliance with **Know Your Customer (KYC)** and **Anti-Money Laundering (AML)** regulations, and is most commonly used for remote onboarding and account opening applications.

KNOW YOUR CUSTOMER (KYC): A set of global guidelines and regulations for the mandatory process of identifying and verifying the identity of a client when opening an account and throughout the customer lifecycle.

ANTI-MONEY LAUNDERING (AML): A set of global laws requiring that regulated entities implement measures to detect and prevent suspicious financial activities.

BIOMETRIC BINDING: The act of connecting live-captured biometric data to trusted personal information on a trusted identity credential to verify user identity.

- Account Recovery: A user who has lost access to an account or privilege engages with a relying party or device to regain access. This can take many forms, ranging from recovery codes and call center interactions to in-person recovery processes or fully automated smartphone transactions, providing varying levels of assurance.

As you can imagine, biometrics represent a significant step-up in trust and assurance when it comes to linking a person to their accounts, transactions, and privileges. Biometrics were the missing piece when it came to connecting various identity elements back to the carbon-based lifeform they describe. And, the more identity elements linked to the biological factor that verifies the individual, the greater the level of trust and assurance. Digital identities became more powerful as a result, and in turn, this increased the value of identity elements, not just for relying parties and their customers or users, but to marketers, researchers, governments, and, of course, bad actors.

The core conflict between accurately describing a physical human being in a digital space and outside parties that seek to collect the identity elements of consumers, citizens, business contacts, in both legal and illegal contexts, has brought forth a decade and a half of regulatory evolution, ethical debate, education, and technological innovation. This period is still underway, but new developments in mobile IDs, data encryption, **liveness** detection, and identity element storage are bringing all the players within and dependent on the identity community closer to an agreement on how best to empower end-users with privacy-enhancing identity technologies. And just in time—with the emergence of synthetic identities and deepfake technologies that trade in **counterfeit identity elements** and threaten to destabilize the very foundation of digital identity, enshrining user privacy is essential if we are to realize the promise of digital transformation.

LIVENESS: The quality of authenticity in a biometric. The term is most commonly used in the context of liveness detection software, which is a support technology designed to detect and prevent **presentation attacks** by verifying a live human being is present at the time the biometric is captured. More recently, liveness has been applied to identity documents as well to ensure they are not digital replicas of authentic or counterfeit documents.

PRESENTATION ATTACK: The act of presenting **counterfeit identity elements** to a sensor in an attempt to trigger a false positive signal, enabling a fraudster to wrongfully authenticate a transaction.

COUNTERFEIT IDENTITY ELEMENTS: Biometrics, documents, and metadata that have been created or modified—by digital or physical means—by a bad actor for the purposes of deception or fraud. This includes (but is not limited to) deepfakes, fake IDs, and misleading or altered metadata.

The Mobile Revolution – Apple Launches Touch ID

Before 2013, online security was primarily confined to knowledge-based authentication (KBA) methods, such as passwords, PINs, and one-time passcodes. In high security scenarios, KBAs could be supplemented by physical tokens—something you have, like a card or FOB. This limited application security because things you know and things you have can be shared, stolen, lost, damaged, or forgotten. The use of a passcode or physical key did not prove that the human being using them to assert a privilege (logging into an online account, authorizing a payment, opening a door, etc.) was the actual human entitled to that privilege. If a password was compromised, or a token or card key was stolen, then whoever had the authenticator also had the privileges it granted.

That began to change in 2013, when—after many years of innovation in mobile technology and experimentation with biometric sensor technology—Apple launched the iPhone 5S, which featured Touch ID: a fingerprint sensor embedded in its home button. It wasn't the first biometric sensor on a mobile phone, but it was the first that was widely adopted, the "killer application" that introduced a third concept to consumer authentication: something you are.

Apple's embrace of fingerprint-based screen unlock popularized biometrics as a convenient way to open a phone, putting fingerprint sensors on the radar of the average smartphone user. Samsung and LG followed course, and within a year, fingerprints were being touted as a password replacement. Software-based face and voice biometrics began to emerge, too, and we started to see a wild west of biometric authentication factors arise.

These were relatively primitive biometrics, however, and severely limited in scope.

The Device Vs. Server Debate

The privacy conversation around the mobile revolution was initially characterized by two privacy philosophies: **on-device biometrics** and **server-side biometrics**. The debate boiled down to this:

- One side argued that because biometric data is uniquely valuable, access to that data should be severely limited; therefore, it should remain only on the **secure element** of the user's device to whom it belongs. All biometric matching should be on-device only.
- The other side argued that without connection to a **system of record** outside the transacting device, a biometric was insufficient for proving identity.

In short, the most privacy-enhancing option—on-device only—lacked sufficient identity elements to form a digital identity, while the more versatile solution for digital identity—centralized server-based—was considered too insecure. This debate raged on for the better part of a decade, but as technologies evolved alongside our understanding of what data is required for a trusted

ON-DEVICE BIOMETRICS: Biometric authentication solutions in which enrolled identity elements are stored and matched in a secure element and never leave the smartphone, computer, or smart card they're on.

SERVER-SIDE BIOMETRICS: Biometric authentication and verification solutions in which enrolled identity elements are stored and matched on a centralized server. This requires secure transmission of biometric data between the sensor and the server.

SECURE ELEMENT: A cloistered part of a mobile device or computer system that applications or network features cannot access.

SYSTEM OF RECORD: A database of foundational identity elements maintained by a trusted organizational body, like a government or educational institution.

identity transaction, a hybrid paradigm emerged that enabled a decentralized approach to biometric processing, with assurance provided by a system of record. This approach would eventually become central to the next-generation mobile IDs of the 2020s, discussed in the privacy solutions section of this report.

NSA's Prism Program

The privacy debate around consumer biometrics coincided with one of the first modern digital privacy scares, when Edward Snowden leaked information on the NSA's PRISM initiative (no relation). PRISM was a top-secret program ostensibly set up to collect data for national defense purposes. Snowden's leak exposed highly invasive data capture and sharing of US citizens' PII. While this had no direct relation to consumer biometrics, the high-profile nature of the PRISM leak, combined with the timing and novelty of technologies like Touch ID, created a flashpoint of paranoia and misconception. Thanks to the participation of tier 1 American technology and telecommunications companies in the NSA's program, a public fear of biometrics being stolen from iPhones marred the excitement of smartphone-based biometrics, even though Touch ID, the most popular consumer biometrics at the time, was on-device only.

While fears that the NSA was harvesting biometric data were based on a misconception, the related privacy concerns over the collection and storage of biometric data were valid. This validation came in the form of a 2015 data breach at the US Office of Personnel Management (OPM), which resulted in the compromise of 5.6 million fingerprint records stolen by hackers. These records included a slew of other identity elements, including social security numbers, names, addresses, health, and financial data. At the time, mainstream media focused on the irrevocability of biometric data, noting that fingerprint images cannot be reset. Identity industry leaders were quick to highlight that the OPM had violated the most basic principles of secure data storage, as the data was unencrypted and fingerprint images, not biometric templates, had been stored. While also emphasizing the need for multifactor authentication, including increasing reliance on biometric verification.

The End of Security

The OPM breach was the canary in the coal mine. In 2017, Yahoo! reported a massive data breach—the largest in history at the time—which affected all three billion user accounts. Biographical, contextual, and transactional identity elements, including usernames, emails, encrypted passwords, and birthdates, as well as account recovery information like security questions and backup email addresses, were all exposed. The fallout resulted in monetary damages of $350 million, sounding the alarm on the nature of user identity data: identity elements are valuable, sought after by bad actors, and inadequately protected.

In the following years, data breaches continued to be reported worldwide. Equifax suffered a breach in 2017, impacting approximately 148 million US citizens, exposing data like Social Security Numbers. A year later, India's national ID program, Aadhaar, was exposed by a security researcher, potentially compromising the biographical and biometric data of over 1.1 billion people. In 2019, Facebook and Capital One each suffered a breach. Then at the dawn of this current decade, LinkedIn, Syniverse, Epic Games, Ticketmaster, and the Shanghai Police all followed suit with significant data breaches of their own.

The result was a perforated security landscape in which user data could not be considered secure. The companies that suffered these incursions took hits to their reputations and their bottom lines, but many of the end users whose data was compromised were impacted far more gravely. The Identity Theft Resource Center (ITRC), which tracks the business and consumer impact of identity theft enabled by data breaches, reports that many victims of identity theft consider suicide.

Strong authentication methods like biometrics began to be adopted to prevent these types of incidents. However, the ongoing widespread use and trust in more sophisticated and resilient identity technology require a concerted effort to strengthen user privacy alongside access control.

Right in the Face

Fast-forward to 2020, and enterprise **digital transformation** received a massive Black Swan inspired boost due to the COVID-19-driven need for remote authentication. The global shutdown of in-person commerce led to an explosion of biometric binding use cases, spawning an unprecedented outpouring of biometric identity innovation. Established identity players that had previously limited their offerings to traditional KBA and DBA authentication, along with established biometrics players, and a surge of hungry start-ups, offered biometric-based solutions to this new identity verification challenge of conducting public and private sector business remotely online.

DIGITAL TRANSFORMATION: The organizational process of integrating digital technologies and procedures into daily operations to increase efficiency, enhance accessibility, and boost customer experience.

While these solutions varied in terms of capabilities, user experience, deployment complexity, and several other factors, they all shared a similar approach to verifying an individual's identity through biometrics. They combined biometric face capture, most often via a smartphone, and matching technology (sometimes on device and sometimes on a server) with **optical character recognition (OCR)** and **computer vision,** enabling software to compare a human face to the picture on an individual's existing government-issued identity document, including passports, national IDs, and driver's licenses.

OPTICAL CHARACTER RECOGNITION (OCR): A class of computer vision technology that enables the reading of text on documents via a connected camera on a smartphone or computer.

COMPUTER VISION: A class of artificial intelligence that emulates object recognition through connected cameras.

The addition of documents into the identity equation introduced another trusted human element, enhancing security in the digital space. But, along with the increased collection of identity elements, there was a growing need to protect them as the pace of data breaches accelerated. And soon, there would be consequences for those who failed to take this task seriously.

The Mother or Regulations

Parallel to the mobile revolution and the tidal wave of data breaches in the mid-to-late 2010s, the European Union was developing a regulation to protect citizens' data. The **General Data Protection Regulation (GDPR)** was in draft form as consumer biometrics began to gain traction in 2013. By May 2018, the regulation had become legally binding in the EU, meaning that any company worldwide handling data of a European Union resident was required to comply with its standards, which remain among the strictest on the planet to this day.

GENERAL DATA PROTECTION REGULATION (GDPR): A European privacy law that came into effect in 2018, granting citizens rights over their personal data. The strict nature of GDPR and its focus on empowering end-users have been a strong foundational influence on similar consumer data protection and privacy laws around the world.

Under the GDPR, individuals residing in the European Union benefit from clearly defined data privacy rights, while relying parties that collect, process, store, and manage user data must adhere to key principles. Individuals must give explicit consent before their data is processed. Once it is, they have the right to easily access, edit, and transfer that data, or even have it erased under the regulation's "right to be forgotten." Relying parties, meanwhile, need to be transparent, legitimate, accurate, and accountable in their data management, lest they be subject to GDPR's penalties for non-compliance: up to 20 million Euros or 4% of global annual revenue (whichever is greater).

It was the law that signalled the rewriting of millions of privacy policies, and while it caused no shortage of headaches in terms of organizational change, the GDPR stands as the example of how to communicate the importance of protecting privacy.

The American Privacy Acts

In the United States, where GDPR effects relying parties but does little to protect end users, two privacy acts with very sharp teeth picked up the slack. Illinois' **Biometric Information Privacy Act (BIPA)** predates the mobile revolution by five years, making it a sleeping giant as fingerprint and face recognition gained traction in security, access control, time and attendance, and surveillance applications. The law demands consent for every instance of biometric collection and disclosure, specifying why it is needed and for how long. The penalties have proven an existential threat to companies that run afoul of BIPA, with individuals able to recover $1000 in damages for negligent violations and $5,000 for reckless violations. The fines were originally per instance, so in cases where employees used biometrics multiple times a day, or had their faces scanned regularly, the ticket multiplied at a frightening rate. In 2024, the law was revised to allow repeated collections of the same biometrics to be counted as a single offense, thereby reducing the potential for massive fines.

BIOMETRIC INFORMATION PRIVACY ACT (BIPA): A 2008 Illinois privacy law concerning the collection of biometric data. Infamous for its heavy penalties, BIPA has led to landmark settlements in the wake of the mobile revolution, as biometrics have become increasingly ubiquitous.

While BIPA is a state-level law, it represents a landmark piece of legislation that, while a thorn in the side of companies that like to play fast and loose with compliance, further illustrates the importance of protecting identity elements like biometrics.

In California, a broader privacy act took effect on January 1, 2020. The California Consumer Privacy Act (CCPA) is the most significant privacy law in the United States and has served as the model for other legislation throughout the country. As essentially the American counterpart to GDPR, the California law empowers end users with rights regarding the transparent collection of their data and the ability to opt out of data sharing, limit its collection, and even have it deleted.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA): One of the first successful privacy laws modeled after GDPR. Like its European counterpart, CCPA formalizes end users' rights to own, control, and delete their personal data.

Children of GDPR

Over the past five years, the rest of the world has followed the example of the European Union and California, enacting GDPR-inspired regulations. Many of these children of GDPR are in regions characterized by high levels of digital identity technology in their private and public sectors. In Brazil, where biometric digital identity technologies are used for shopping, banking, and pension collection, the LGPD (General Personal Data Protection Law) came into effect in 2021. Meanwhile, India, which boasts the most expansive biometric national ID program on the planet — the Aadhaar (Unique Identification Authority of India) —is building a legal framework for personal data protection in a similar vein. The UK is also making headway in its own post-Brexit privacy legislation.

Forty-six out of 54 countries in Africa have a form of legislation governing privacy, many following the key ideas set forth in GDPR. The Asia Pacific region has diverse privacy laws, with Japan and Singapore showing clear signs of inspiration from EU law, and China making significant strides in enabling data sovereignty. Indeed, with privacy laws on every continent either in effect or undergoing rapid development, it's clear that compliance with data protection is no longer optional. The time for racing ahead of regulation in the name of profit and innovation is over. It's time to protect privacy and achieve compliance, or face the penalties.

Next Generation of Privacy

So, we know the situation: personal data, especially identity elements, are valuable and vulnerable. Lawmakers from around the globe have recognized this and, following in the footsteps of the European Union, have established regulations to protect user privacy and limit data exploitation by third parties, whether malicious actors, unscrupulous corporate entities, or even public organizations that are lax in their oversight. We need technologies that enable compliance and protect privacy, while still enabling the convenience and automation promised by digital transformation. Thankfully, the leaders in biometric digital identity have been working tirelessly to create innovative solutions that put users in control of their identity elements in ways that are naturally compliant with privacy laws in digital and physical contexts.

From **mobile IDs and mobile driver's licenses (mDLs)** to innovative encryption and storage solutions, like those offered by Privacy Paragon Anonybit, to widely available **passkeys**, to digitally signed biometric barcodes and on-demand, ephemeral biometrics—biometric digital identity solutions have continued to evolve. And while the regulations may change, the core concepts of privacy and identity remain the same. With the alignment on display from the global privacy community, relying parties seeking solutions for identity data protection will be best served by vendors that prioritize the protection of user data.

MOBILE ID/ MOBILE DRIVER'S LICENSE (MDL): A digital credential securely stored on a smartphone. The best mobile IDs and mDLs are validated against a government system of record, allowing users to control which identity elements they share on a transaction-by-transaction basis.

PASSKEY: a passwordless credential based on standards set forth by the FIDO Alliance. Passkeys allow users to sign in to apps and websites using device unlock mechanisms on their computers and smartphones. Because they are device-based, passkeys are privacy-by-design.

Where We Are Now

This brings us to our current moment in biometric digital identity, where relying parties are seeking solutions to help secure and protect identity in their digitally transformed businesses. And those solutions need to be compliant and privacy-first, not only because regulations demand it, but because, as we will see in this report, digital identity only works if bad actors can't hijack the identity elements that belong to the users.

The Prism Project Reports and Sponsorship Opportunities

Showing Identity in a New Light

The Prism Project arose organically out of a collaborative survey-based research project launched by Acuity Market Intelligence and FindBiometrics in late 2022. The intent of the Project is to use the proprietary Prism framework as the lens through which we continue to analyze and evaluate the rapidly evolving biometric digital identity industry as we help influencers and decision makers understand, innovate, and implement digital identity technologies.

Published Reports

In 2024 and 2025 The Prism Project published seven reports, focused on biometric digital identity adoption in key vertical markets and the major threats facing the industry:

- The Financial Services Prism Report
- The Travel and Hospitality Prism Report
- The Government Services Prism Report
- The 2024 Flagship Prism Report
- Deepfake and Synthetic Identity Prism Report
- Privacy and Compliance Prism Report
- The 2025 Flagship Prism Report

2026 Sponsorship Opportunities

The Prism Project will publish, promote, and distribute two new Full-Spectrum reports in 2026, focusing on the financial services sector and the next evolution of biometric digital identity:

- The 2026 Financial Services Prism Report
- The 2026 Flagship Prism Report

Additionally, we will be introducing new Focal-Point Reports: shorter, sharper reports that laser-focus on flashpoint issues in identity, like:

- Airport customer journeys

- Agentic AI
- Gaming
- Decentralized identity

Download our 2026 brochure for more information.

Ongoing Collaboration

The Prism Project is conducting on-going research and continuing to explore how biometric digital identity is being used today, where the roadblocks to adoption lie, what obstacles must be overcome to successfully deploy these technology solutions, and where they are being used and by whom. We welcome collaborators and are open to discussing how your organization might benefit from and/or leverage the opportunities The Prism Project presents. To reach out, visit www.the-prism-project.com or email us at info@the-prism-project.com.

About the Author

Maxine Most

Internationally recognized biometrics and digital identity thought leader celebrated for provocative market insights, accurate market predictions and forecasts, and unbiased, pragmatic market intelligence.

Strategic innovator, market visionary, and forecasting guru Maxine Most is the founding Principal of Acuity Market Intelligence (www.acuity-mi.com), a strategic research and analysis consultancy recognized as the definitive authority on global biometrics market development. Throughout her decades long career, Maxine has evangelized emerging technology on five continents. Since 2001, she has applied her unique ability to bring clarity to the unpredictable and volatile world of emerging technology to the rapidly evolving biometric and digital identity marketplace.

As an executive strategist, Maxine has earned a stellar reputation for innovative thought leadership by consistently providing unique, unvarnished, and reliable market insight while accurately anticipating biometric and digital identity market trends. Under her leadership, Acuity has provided strategic guidance to Global 1000s, established technology market leaders, start-ups, and a range of organizations in between. Most leverages her deep understanding of technology evolution, emerging market development, and the process through which industry leaders are created to provide candid strategic analysis, highly targeted implementation plans, and quantifiable, measurable results.

Ms. Most is the author of numerous biometric and digital identity research reports including Face Verification & Liveness for Remote Digital Onboarding," "The Global Automated Border Control Industry Report: Airport eGates & Kiosks," "The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy," "The Global National eID Industry Report," "The Global ePassport and eVisa Industry Report," and "The Future of Biometrics," as well as a contributor to several books including "Digital Identity Management" edited by digital identity thought leader David G. Birch.

Ms. Most regularly offers insight and analysis in on and off-line publications, is quoted often in industry, business, and consumer press, is an active contributor to the Kantara Initiative, and presents regularly at industry events on the evolution and development of biometrics and digital identity markets. She is a graduate of the University of California, San Diego with a multi-disciplinary degree in Mathematics and Computer Science and minors in Visual Arts and Economics.

Let The Prism Project be Your Guiding Light!

The Prism Project (www.the-prism-project.com)
The Prism Project is an innovative framework for understanding and evaluating the rapidly evolving biometric digital identity marketplace is **the only market model that is truly biometric-centric** based on the foundational conviction that in the age of digital transformation the only true, reliable link between humans and their digital data is biometrics.

Maxine Most
Principal, Acuity Market Intelligence
cmaxmost@acuity-mi.com
Founder, The Prism Project
cmaxmost@the-prism-project

About Acuity Market Intelligence:

With decade of practical expertise in the unpredictable and volatile world of emerging technology, Acuity Market Intelligence consistently delivers consistently original, thought-provoking, and reliable insight and analysis. Proud, self-proclaimed technology business development and marketing geeks, Acuity is globally renowned for its uniquely customized business and marketing strategies and for creating and deploying innovative programs that integrate digital and traditional channels and platforms.

Visit acuitymi.com and let us help your organization thrive.