Identity Technologies: Trends, Drivers, and Challenges

An Industry Discussion

NATIONAL INTELLIGENCE COUNCIL REPORT
NICR 2014-06, 13 August 2014
(U) This is not an IC-coordinated report.

This paper does not represent official US Government views.

Identity Technologies: Trends, Drivers, and Challenges

An Industry Discussion

Executive Summary

All developed nation states are proceeding with physical identity programs, particularly with research and development (R&D) in academic institutions. Besides the United States, some other major players are China, Germany, and the United Kingdom. Privacy concerns are not as prevalent in some other countries, so they have the potential of outpacing the technological developments of the United States.

Users are in the early phases of managing their virtual identities; both the number of online identities and the sophistication of how one maintains and curates such identities are increasing. The concept of virtual identity continues to evolve as more information is digitized and becomes available via the Internet and other online services.

As analytics evolve and various aspects of data are aggregated and correlated, the capabilities of data scientists will become increasingly important. Equally important are the skills to cultivate analytic outputs that have not already been explored, especially in genomics research.

Understanding the relationship between physical and virtual identities is becoming more important, especially as it becomes more commonplace to use one's virtual identity to conduct business in the physical world. Many younger users are savvier at maintaining multiple online identities, which might or might not correlate to their physical identity.

- Preventing spoofing and guaranteeing a positive identification in the virtual space that correlates to a specific physical identity are difficult.
- Convergence of physical and virtual identities will authenticate certain online transactions and communications. However, some people might wish to keep their virtual identities separate and distinct from their physical identities, due to privacy concerns.
- The identity associated with a technical platform might or might not be separate from the user—a device can have multiple physical and virtual identities linked to it.

This paper does not represent official US Government views.

Contents

This report was prepared under the auspices of the National Intelligence Officer for Cyber Issues and drafted by the NIC.

This paper does not represent official US Government views.

Discussion

The following commentary represents the professional views of private sector experts working in the identity technology industry; it is not intended to be a comprehensive study of the subject matter.

Physical Identity

Trends

All developed nation states are proceeding with physical identity programs, particularly with research and development (R&D) in academic institutions. Besides the United States, some other major players are China, Germany, and the United Kingdom. Privacy concerns are not as prevalent in some other countries, so they have the potential of outpacing the technological developments of the United States.

- Some countries, such as India, are already using biometrics as part of their national identity system for access to government services.

US companies are concerned about protecting their intellectual property (IP) and ensuring timely payment for products and services. One solution involves keeping IP within the software—where it is easier to control—rather than in the hardware. Sometimes components are added to products that do not do anything; they are simply included to confuse those trying to steal IP.

In the United States, physical identity technology is generally export controlled, i.e. devices developed within the United States are not allowed to be sold to certain countries. Technology is still being developed in these countries, but it is not based on US technology.

- Indian researchers are using open-source information to develop physical identity technology for use in key markets untapped by the United States. However, entering the Indian market is difficult because Indian regulations require domestic manufacturing.

Industry experts judge that during the next four years, advances in physical identity scanners linked to mobile phones will provide first-level authentication for device use and online services. Some mobile devices use a fingerprint scanner to unlock the hardware. In the future, tying a scanner to a bank authentication and using a fingerprint or other biometric feature to submit payment might result in one no longer needing to carry credit cards or multiple forms of identification. The technology is not lacking, just people's willingness to use it.

- This capability already exists in Africa where mobile phones are widely used for banking transactions.

- Hospitals might also use physical identity technologies to establish or validate identification.

Facial Recognition. Although facial recognition has been in use for years, it still requires human review for accurate evaluation. Large-scale facial recognition—such as the use of closed circuit television (CCTV) cameras in London—is an expensive technology that has had mixed reviews. It will not be successful unless it is used frequently and the results are tracked. Consistent data formats and the collection of high-quality images are also necessary.

Companies, such as casinos, look for opportune camera placement locations. Requirements for favorable imaging include specific angles and good lighting. Stairways, halls, escalators, and other high-traffic areas are good places for cameras in casinos. In addition, social engineering techniques can be employed to get people to look toward the cameras, including

flashing billboards and mirrors, which provides better, front-shot images for facial recognition. Algorithms then compare images with data already stored or exchanged with other casinos.

Social media companies are developing and employing advanced facial recognition technology. However, many consumers do not realize how these websites are collecting and processing physical identity information. People are under the impression that their uploaded photos are just being viewed by their friends.

- The German Government required this practice to be discontinued for its citizenry due to privacy concerns.

- Use of facial recognition by social networking mediums will dominate the market during the next four years. However, data precision will be less for general-use applications than for applications used by the US Government for law enforcement purposes.

Fingerprinting. Fingerprint databases all use surface print images, which will not likely change for the foreseeable future. Market demand is minimal for the enhanced development or use of subdermal imaging technology or databases. However, demand does exist for higher-resolution, latent print matching (for the fragmentary impression of a finger), which accounts for only a small part of identification.

Separately, a very small market exists for higher quality in palm scanning technology. However, because palms provide extensive data, produce large images, and require larger imaging devices, opportunity for commercial growth is limited.

Iris Recognition. Better imaging resolution in iris scanning is a pressing need. Each vendor has established its own standard, but an international industry standard is needed that provides for an objective evaluation of image quality. In addition, a methodology is needed to evaluate the quality of images and also objective criteria for acceptability of images.

Iris recognition R&D is becoming very common in Chinese universities, some of which have large databases of iris images. Chinese universities are making great strides in iris research, and one should expect a significant increase in their commercial offerings of low-cost devices, even in the United States. Chinese reverse-engineering of US iris recognition technology is also occurring.

- For example, China is able to take US iris recognition technology and recreate it at 80-percent quality and at lower cost.

Genetics. As the technology moves from phenotype to genotype, more genotypic markers will probably be captured, enabling population studies and trend analysis. Although people are getting genetic testing, the sample set is not large enough to prepare population studies. As people understand the medical research benefits from large population studies, which track diseases as they cross borders, this technology will greatly improve.

- Applied technology in forensics has been increasing. Western Europe is conducting some testing in this area.

- In the next four years, distinguishing identical twins will be trivial.

- Genomics shows promise for mapping regional disease patterns, although this task would require large quantities of data. Once a database of genomic information on thousands of people is assembled, one could better understand regional inheritance and disease patterns.

- In addition, combining social media with genomics might enable the identification of personal remains after accidents or natural disasters—if the database were large enough.

Genomic data might have even more uses later, which supports the argument to collect more now for future utilization.

Genomics is prominent in China; Beijing Genomics also has a presence in the United States. Germany, Italy, and the United Kingdom, which has the Sanger Institute, are also prominent. All of them are ahead of the United States in understanding population genetics.

- Saudi Arabia is also examining the use of genetic markers for disease identification.

Drivers

Industry experts assert the major market drivers for physical identity technologies include: (i) availability of cost-effective and user-friendly solutions, (ii) consumer demand for daily use, (iii) ability to integrate physical identity solutions into mobile devices, (iv) ability to integrate stronger algorithms, and (v) leveraging "cloud-based" capabilities.

- Usability of physical identity technology systems is a primary factor driving development. The systems must be easy to use and automated so that the data are usable across platforms with the widest range of physical identity technologies collected and the best quality images and templates captured. Cost of the systems, and cost-effective results, are important too, although cost ultimately depends on the application and expectation of performance.

- Proliferation is also important, and good pilot programs are crucial. The population needs to be motivated to accept the technology by showing the benefit of the applications.

Challenges

Industry experts judge the major challenges to improved physical identification include: (i) gaining public trust regarding privacy and security, (ii) increasing user acceptance of "consumer grade" physical identity technologies, (iii) managing data complexity to meet the analytic speeds desired by consumers, (iv) expanding storage capacity (particularly for human genomes), and (v) meeting the price point consumers are willing to pay. In addition, the experts also identified some specific technical, societal, commercial, and governmental obstacles.

Technical. Some users with access to physical identity scanners will try to hack or defeat the systems. With greater access to devices, they will have more opportunities to spoof the technology. The challenge to industry will be countering the countermeasures.

- Internet videos explain how to "crack" fingerprint scanners on mobile devices.

- One business risk related to iris recognition is new patterned contact lenses, which hinder the ability to discern features of an iris.

- DNA spoofing (i.e. shedding hair or skin cells) is a disrupter that might negatively impact the effectiveness of identity recognition and verification. Surreptitiously collecting some types of DNA samples from anyone (e.g. people sitting in a room who leave behind many DNA markers) is relatively easy.

Societal. Societal challenges outnumber the technological challenges in the evolution of the physical identity industry. Physical identity technology will have to be widely used by the public to overcome social challenges and privacy concerns.

- Although the United States is the leading innovator of physical identity technologies, privacy concerns and reluctance of the populace to fully embrace physical identity technologies might result in other countries

outpacing the United States, especially for use by the public sector.

Commercial. Traditional physical identity companies cannot survive in the business environment in 2014 and have mostly been acquired by larger companies that have massive volumes of data needed to test these technologies and capitalize on them. These huge data providers can advance physical identity as a byproduct of their other business operations.

- Initially, only a few vendors pursued this technology, and they would only license to certain agents.

- A new business environment is evolving as companies decentralize their operations geographically or outsource data services. Cloud computing and distributed processing power contribute to this decentralization.

Vendors of physical identity technologies have marketing and advertising problems. Industry needs to be more open with the public about technical limitations and counter the belief that physical identity technologies are infallible.

Governmental. Government regulation and requirements impact physical identity technology development. Governments possibly focus too much on security and defense-related concerns to the detriment of R&D for commercial applications.

- Some technological development is driven by government requests, and the transition to a corporate vision focused on commercial markets is difficult for many US-based companies.

Politicians and the media need to be better educated about the accuracy of the technology in order to overcome paranoia while also setting realistic expectations on its use. The social media atmosphere also creates its own challenges, especially if mistakes occur during technology rollout. The public needs to be made aware of the capabilities of the technology and informed that it is not fail-proof.

Virtual Identity

Trends

People are in the early phases of managing their virtual identities; both the number of online identities and the sophistication of how one maintains and curates such identities are increasing. The concept of virtual identity continues to evolve as more information is digitized and becomes available via the Internet and other online services.

Authentication. Users are frustrated with maintaining multiple accounts and passwords. Leading R&D technologists are seeking ways to compile online identifications and compartmentalize specific parts of virtual identities (e.g. brokerage and bank identifications). Composite methods and continuous modes of authentication are expected, as well as a multitude of algorithms that will be absorbed into the marketplace.

Authentication protocols across all platforms and operating systems will become more important. As protocols get absorbed into the fabric of the Internet (e.g. browsers and operating systems) and get used as a building block for other purposes (e.g. e-commerce systems) the question will be how to enable a flexible yet strong identity. The flexibility requirement stems from the need to be agile across multiple systems with a high level of assurance.

Device fingerprinting, or linking devices for partial authentication, will not be eliminated anytime soon. That process entails both active and passive identity—including touch gestures, keypad typing, and other latent indicators—in addition to traditional authentication tools.

- These devices do not provide positive digital identification; rather, they provide a threshold level of confidence that is acceptable for authentication. The machine gives a score and decides whether or not to permit any transactions with a certain device.

Attestation is the requirement to prove that information comes from a trusted source. Web administrators request that a device or user attest itself, although on what scale is still unknown. Cloud computing enables smaller businesses to do more significant computing because they do not have to install or maintain their own systems.

- This same idea will be used to determine an economy of scale for security—cloud-based security and attestation services enable users to have a much better opportunity to of defend themselves from attacks. In the past, this concept was used to detect credit card fraud.

- The discussion of a single sign-on has been going on for years. If two applications require the same attestation from a user and agree on the granting authority of that attestation, then a single process should suffice. A network-based sign-on at the network level instead of the user level is also a possibility.

Data Science. Data science—using big data to make evaluations that can be applied to multiple problems—will expand. Professionals with computer science backgrounds will be needed that possess the ability to maintain data sets and authenticate accesses. Decisionmaking will evolve so that data science is applied and enhanced via virtual identity information.

- One example would be using a data-science approach to determine which cases lawyers would likely take.

During the next four years, the potential for the connection of proprietary content to social media data will increase. Connection of passive and active virtual identity data might become more commonplace (e.g. combining credit reports and social media).

Advanced Analytics. During the next four years, big data analytics will become more efficient as more processing power is packed into smaller devices, and as new technology is implemented into those devices (e.g. the ability to recognize faces and track people). The capability exists for some major online vendors to be able to confirm package receipt by combining drone technology with facial recognition—assuming the vendor possesses a picture that is associated with the name.

Machine-learning might also become more prevalent. Improvements have been made over time in machine-learning, yet most people using digital applications do not realize they are contributing to the process.

- Tagging photos is helping machine-learning by refining and perfecting algorithms and statistical methods.

- Voice digital assistant applications are proceeding towards the goal of a smart machine.

Drivers

Industry experts assert some specific major market drivers impacting the development of virtual identity technologies include: (i) the ability to include geographic data with consumer activities, (ii) increased interest in raw social data combined with other data sets, (iii) local users' control on their own data and its derivative use, (iv) real-time access to content, (v) consumer desires for advanced image processing, (vi) the convergence between consumer and business identities, and (vii) user desire for cross-device transparency. The general topics of anonymity, control, and trust were also highly prevalent.

Anonymity. A desire for consumer anonymity in the online social and digital environment is driving development. Users want the ability to obfuscate their online activity—to choose what will be attributable and what will remain anonymous across multiple online accounts and activities.

- Systems such as The Onion Router (TOR) and some digital currencies have been built to avoid monitoring and enable users to operate anonymously online.

Another driving factor is the development of obfuscation techniques so that users can create rules to allow certain other users to access their information. The majority of users do not want liability for maintaining or protecting data, but they will allow algorithms and software applications to take over in business practices.

Control. Users want more control; they want to control what information is available publicly about them and how others get to use it. Personally identifiable information (PII) is usable by many leading social networking providers.

- People want the ability to sell their own PII, if they choose to do so.

- Often, people accept the terms of use for websites because they want some benefit, usually a free online service. However, they fail to realize or forget what is being given up in the process. For example, one video streaming service has more than 100 pages of terms and conditions, but whether anyone reads them before signing up for the service is questionable.

- Data analytics have the potential to reveal the inherent value of what people are giving up. As a result, they might start to demand new types of online services.

Trust. Users are becoming increasingly aware of different types of data sharing. If users became apprehensive about how their personal data is being used, they might be inclined to leave the application. Maintaining a steady platform and active users is imperative for social media groups and applications to remain relevant. Also, the virtual identity industry needs to determine what user expectations are with different platforms and be flexible to those needs and expectations.

- For example, even if someone donated blood to help with a natural disaster, he might think twice about donating blood so that an insurance company could set insurance rates for a market demographic.

- Maintaining a certain degree of trust between users and keeping accounts active is imperative for interacting with social media groups and applications.

Challenges

Industry experts judge the major challenges to better virtual identification include: (i) public trust regarding privacy and security, (ii) legislation not maintaining pace with technology advances, (iii) public perception of how information is used, (iv) sustainability of data quality and validity, (v) limited identity and access management solutions for “cloud based” solutions, (vi) anonymizing technologies, and (vii) the ability to verify persons through enrolled biometrics.

Legislation. Technology develops where money is to be made (e.g. in the entertainment industry) and is often years ahead of any country’s relevant legislation. New legislation is being considered in numerous countries, including the United States, to address anti-theft capabilities for mobile devices. The proposed statutes would require that a device “knows” who the user is, requiring all users to provide PII linking them to their devices.

- The National Institute of Standards and Technology (NIST) is conducting extensive work in this area, but its success depends on

the accuracy of the underlying data. Despite the quality of NIST's efforts, technical issues remain with these systems and protocols.

- Nationalization of encryption protocols is another legislative option under consideration. However, it might prove ineffective because the Internet does not respect geographic boundaries.

Aggregation and Convergence

Aggregating and Correlating Various Aspects of Identity

As analytics evolve and various aspects of data are aggregated and correlated, the capabilities of data scientists will become increasingly important. Equally important are the skills to cultivate analytic outputs that have not already been explored, especially in genomics research.

- For example, employing data analytics with certain identifiers, such as date of birth, zip code, and one other data point, enables a more advanced authentication regime.

- The combination of genomics data, ancestry or lineage databases, and social networking services utilizing physical identity information might increase confidence in analytic evaluations and enable pre-emptive screening or treatment of regional, genetically linked health issues.

Physical identity technology will increasingly move from work spaces, to home, to mobile devices and might be associated with various profiles. Differences will emerge between government and corporate environments and consumer systems at home.

The ability of companies to connect all of one's social networking data and sell them is becoming easier. Advertising agencies are aggregating and correlating online information, enabling the unintended aggregation of identification data in some instances.

- For example, when a person buys a book on Alzheimer's for a neighbor, that transaction is linked to the purchaser.

- On the other hand, companies do not have to know a person's identity if they know his or her friends; they still might be able to aggregate data about that person based on social and family ties.

- One social media provider prohibits aggregation of data from other networks and applications, and some information providers have sought control over the resale of data they provide.

Companies often fall into the dilemma of trying to get as much data as possible, sometimes maintaining data that they should not. This situation might lead to customer dissatisfaction.

- Service providers might not really care about the users' physical identity; instead, they might just care about vetting critical elements of data—such as the behavioral patterns associated with a credit card.

- Aggregation of PII from international sources might also have implications for US entities. Some data can be aggregated from devices or users operating abroad, regardless of an individual's home country or where a company is registered.

Accuracy. In order to ensure that the data are accurate, one must find ways to scrub them for inaccuracies. Marketing and analytic firms are developing mechanisms to determine which information is real and false.

- For one social media provider, 40 percent of new accounts are created by bots, which pass

around information. However, no one is willing to assume liability for bad data.

- An industry is emerging whose purpose is to clean and filter data. Generally, a vendor is more concerned with the accuracy of the data if it sells expensive products or provides professional services.

Convergence Between Physical and Virtual Identities

Understanding the relationship between physical and virtual identities is becoming more important, especially as it becomes more commonplace to use one's virtual identity to conduct business in the physical world. A physical person directly or indirectly created every virtual persona, so the connection between physical and virtual is inherent—even if it is a fake identity.

- Many younger users are savvier at maintaining multiple online identities, which might or might not correlate to their physical identity.

- Some people have a different image or persona at work than with their family. As such, one needs to have a better understanding of the relationship that connects the physical and virtual identities.

Convergence between virtual and physical identities is not necessarily so. Interactions between users will dictate how and to what degree the two converge and influence trust. Users need to be contextually aware to manage the relationship.

- Virtual identity will become increasingly important to control because more and more of one's daily life activities will be done with one's virtual identity. Physical identity is a powerful way to exert control over one's virtual identity.

Positive Identification. Preventing spoofing and guaranteeing a positive identification in the virtual space that correlates to a specific physical identity are difficult. Convergence might add a higher degree of accuracy to certain databases.

- Adding a physical element, for example, associating a fingerprint with the online identity, would add more identification value to the online presence.

- People might have multiple personal social media accounts, accounts for their kids, and even for their pets.

- Tagging of photos might or might not be accurate.

- These disparities necessitate performing a better identification process when seeking to gain a positive identification.

Convergence of physical and virtual identities will authenticate certain online transactions and communications. However, some people might wish to keep their virtual identities separate and distinct from their physical identities, due to privacy concerns.

- Cultural resistance is less in non-US countries, which presents great opportunities to refine technology advances, given the large volumes of data available for testing overseas.

- The relationships between Chinese social media and physical identities are unknown because testing them from outside China is impossible. More specifically, the geographic restrictions that China places on uploads and proxy server use inhibit meaningful evaluations.

Experts from the virtual identity industry assert the convergence of virtual identity and physical identity is a complicated and intricate process.

Virtual identity is an evolving definition. As an example, no one has determined if the scope should be limited to oneself or if it should also include one's surroundings. The ecosystem around people provides insights into their behavior patterns and might be used to determine their eligibility for certain products or services (e.g. credit card interest rates). These considerations raise concerns about privacy and individuality.

Device Identity. The identity associated with a technical platform might or might not be separate from the user—a device can have multiple physical and virtual identities linked to it. Two options exist: either a device is owned by a user that has that physical identity attached to it (e.g. a registered mobile phone) or the device is user-independent (e.g. a public pay phone).

- Some products accept a smartphone or smartwatch as an expression of identity, so the only communication required to validate identity is with the local device.

- Training might be required to ensure that secure device identification does not interfere with the user's normal online experience.

- Once a following gathers in the next couple of years, the facial and iris recognition modalities will likely improve for mobile devices.

This paper does not represent official US Government views.