The University of Texas at Austin
Center for Identity

Current Biometric Adoption and Trends

A UT CID Report
by Rachel L. German and K. Suzanne Barber

May 2018

The Center for Identity greatly appreciates and acknowledges the following organization for their research gift:

TransUnion

Executive Summary

Why Read this Report?

In today's technology-driven marketplace, staying aware of the latest trends in identity authentication is essential. Customers can be courted with convenient and trusted identity verification procedures or driven away by burdensome and unreliable systems. Confidence in the identity of your users is not only a best business practice, but a legal requirement in many cases.

In order to both protect customers' data and provide them with a streamlined experience, companies must carefully consider all of the authentication options available to them. The following trends in biometric adoption can help a business to gain insights into emerging usage and acceptance rates of biometrics across a wide range of applications and markets.

Key Takeways

What types of biometrics are most popular?
Fingerprint scanners are the most common technology used for biometric authentication, with face recognition and iris scanners not far behind.

What are the trends in technology platform (e.g. mobile devices, laptops, on-site) for biometric adoption?
The majority of uses of biometric authentication are performed on-site, but mobile device usage is a fast growing area.

Which market sectors show the most increase in biometrics?
Information technology, finance, and government show the most increase in biometric authentication, with retail and software services close behind.

Which types of consumer activity are targeted by businesses rolling out biometric authentication?
The financial sector has seen an explosion in biometric use, with fingerprint scanners, voice recognition, iris scanners and even heartbeat monitors used by customers to access accounts and make purchases.

Do trends indicate future increase in the adoption of biometrics?
The last five years have seen a rapid increase, not only in adoption, but also in the range of market sectors and targeted consumer activities. Adoption of biometric technologies should continue to accelerate and expand across all user domains and market sectors.

Introduction

We hear about biometrics in many different contexts, from access to our devices to crossing border checkpoints. The word 'biometrics' is derived from the ancient Greek bios (life) and metron (measure). In general usage, biometrics refers to both the methods used to measure and analyze an individual's unique physiological or behavioral characteristics and the characteristics themselves. These include fingerprints, facial geometry, iris patterns and more. Due to this variety of meanings, research in the field of biometrics encompasses a broad realm of activities. Researchers focus on identifying traits that are unique to individuals, developing and testing the reliability of technologies used for verifying biometric matching, and analyzing consumer attitudes towards and comfort with the collection, use, and digital storage of such traits.

Less than a decade ago, consumers still feared biometric applications as clandestine extensions of government and law enforcement. Business initiatives relying on biometric applications once failed across market sectors, but that trend seems to be changing as younger consumer generations are now surrounded by smartphones and wearables. Consumer biometric acceptance and adoption by consumers seems to be changing as more companies use biometrics to identify and authenticate users. In this report, the UT CID team examines several questions related to the adoption of biometric authentication across the consumer and business landscape.

Research on consumer attitudes about using biometric authentication has been mixed. The ease of using a biometric for authenticating your identity in daily transactions is a strong incentive for consumers who are inconvenienced by the need to memorize difficult, secure passwords. On the other hand, studies have found that privacy concerns were a strong influence on consumers' reluctance to use biometric authentication systems.[1] Despite some consumer concerns about the privacy of the biometric data, biometric authentication is a rapidly accelerating market and forecasts predict this growth to continue. Governmental use of biometric to identify citizens for various purposes is increasing alongside consumer trends. According to ABI Research, the biometrics market will reach $30 billion by 2021.[2] Increased smartphone capability is leading much of this growth. Acuity predicts that 4.8 billion smart phones equipped with biometric capability will be in circulation by 2020.[3] With biometrics becoming more ubiquitous and secure, consumers will find increasing opportunities to utilize these new technologies.

---

1 *Clodfelter, R. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? Journal of Retailing and Consumer Services, 17(3), 181-188; Morosan, C. (2012). Voluntary Steps toward Air Travel Security: An Examination of Travelers' Attitudes and Intentions to Use Biometric Systems. Journal of Travel Research, 51(4), 436-450.*

2 *https://www.abiresearch.com/*

3 *http://www.acuity-mi.com/GBMR_Report.php#sthash.RYvEN9VG.dpuf*

In this study, we explore adoption of biometric authentication across types and user domains, as well as industries, platforms, and targeted consumer activities. In doing so, we address the following questions:

- Is biometric adoption really accelerating?
- What types of biometrics are most popular, and in which industries?
- What are the trends in technology platform (e.g. mobile devices, laptops, on-site) for biometric adoption?
- Which market sectors show the most increase in biometrics?
- Which types of consumer activity are targeted by businesses rolling out biometric authentication?
- Do trends indicate future increase in the adoption of biometrics?

Methodology

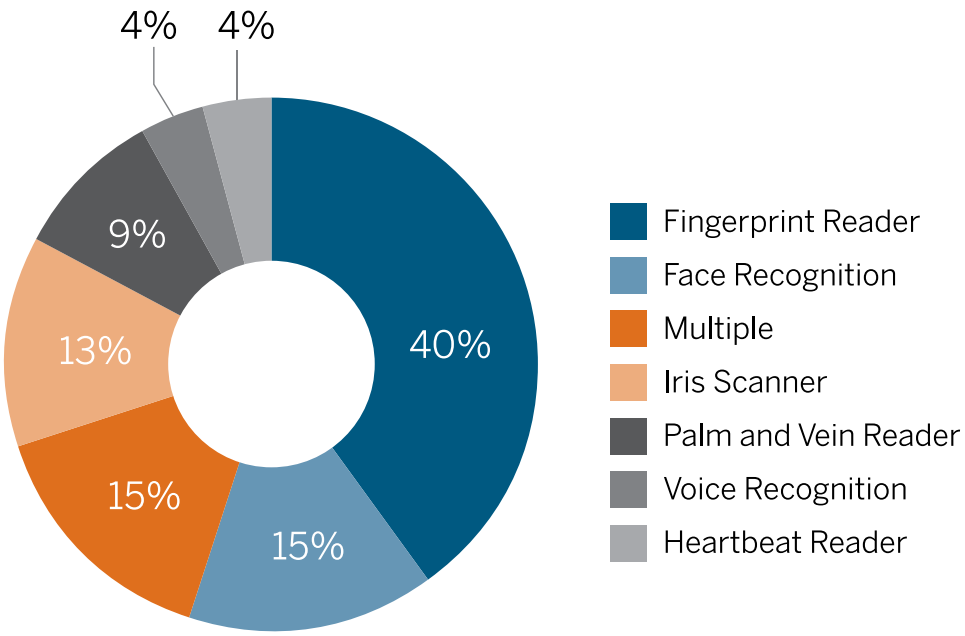
In order to get an overview of the types, platforms, and market sectors in which biometrics are being used in the marketplace, we employed the internet to search and find the most prominent uses of biometrics. Our investigations focused on searches for "biometric technology" and "biometric authentication" to find the most prominent examples of entities using biometric technology to identify individuals between 2004 and 2016. Next, we further narrowed the field by retaining only instances involving media coverage about the release of new biometric applications. Finally, the remaining 53 marketplace and government applications of biometric technology were coded and analyzed in order to describe various aspects of their usage. In this report, we describe the following characteristics of biometric adoption:

- Biometric Types
- User Domains
- Platforms
- Targeted Activities
- Market Sectors

Biometric Types

Various types of biometrics are used for authentication in both the public and private sectors. Figure 1 shows the proportions of applications using each type of biometric. Fingerprints are still most common, used in a wide variety of settings. These include McDonald's and Forever 21 employees for time clock and cash register access, Bank of America customers for ATM transactions, as well as for student purchases at several campus retailers. Face recognition is growing quickly, too, for everything from unlocking mobile apps to searching FBI databases. Some entities use a combination of biometrics. Wells Fargo has implemented a combination iris scan and face recognition for mobile banking. Iris scanning is also used in healthcare services to uniquely identify patients as well as for identifying passengers in major U.S. airports. Palm and vein readers, voice recognition, and heartbeat readers are the least utilized at this time.

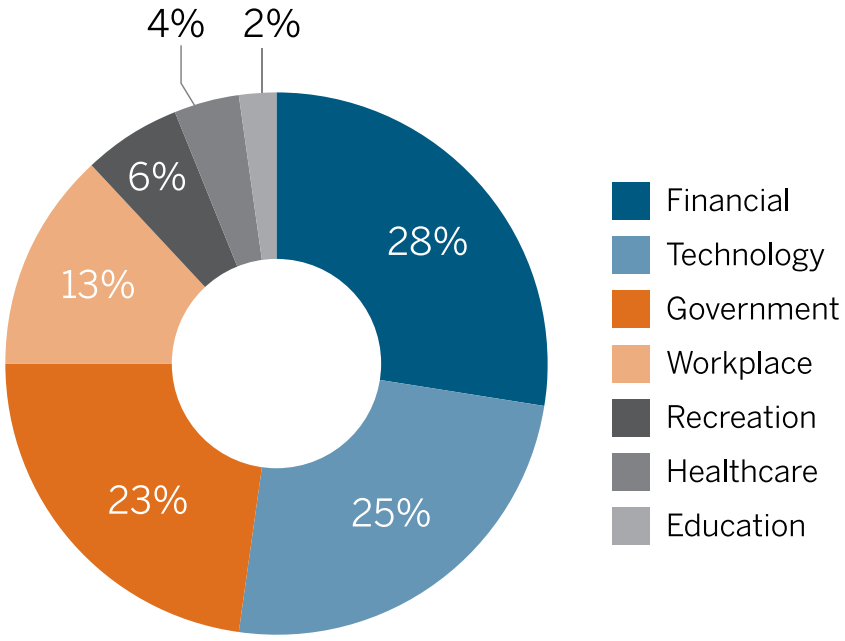
Figure 1.
Biometric Types



User Domains

For our purposes, 'User Domain' refers to the general type of services and activities in which users employ biometrics to identify themselves. This differs from 'Market Sector' in that the user domain is a broad area of activity including workplace and governmental interactions, while market sector refers to the specific industries implementing such technologies. Figure 2 shows the various domains in which individuals are using biometrics to authenticate their identity. Financial services, technology, and government are the top three areas seeing high activity in biometric adoption, while workplace uses are on the rise.

Figure 2.
User Domains

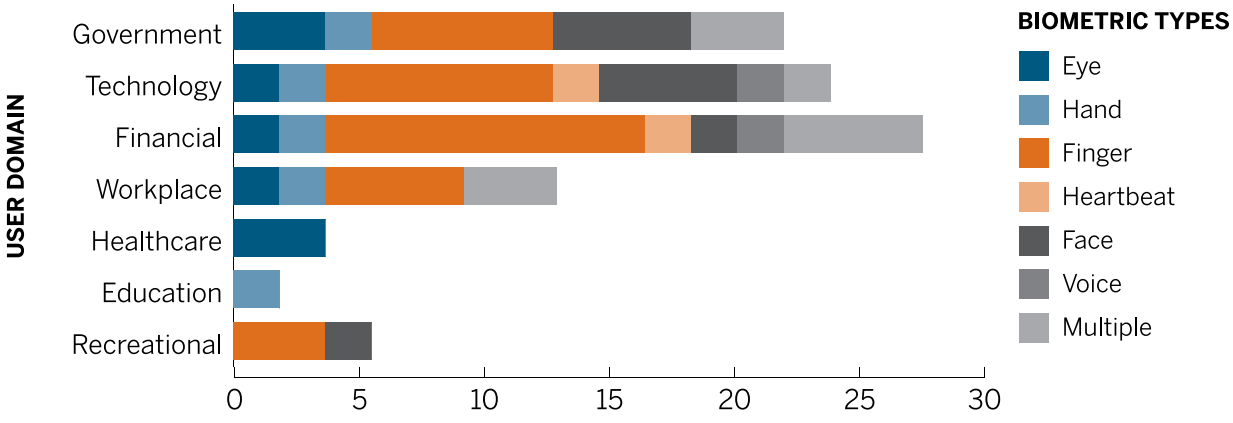


The domain with the highest activity in biometric authentication is financial services. Wells Fargo, Bank of America, Citibank, Mastercard, and others use technologies ranging from fingerprint readers to heart-beat-monitoring bracelets in order to authenticate their customers at ATMS, online, and at the point of purchase. A major contributing factor to mobile biometrics growth is an increasing supply of biometrics-enabled personal devices, including Apple and Samsung's fingerprint scanning smartphones.

Governments across the globe are jumping on board with biometrics for many different purposes. Many nations are using fingerprints or palm readers to identify citizens for voting or receiving benefits. In the US, we find government uses of biometrics that include iris scanning for TSA screening in airports, facial recognition for the FBI database, and fingerprints for tracking inmates in the prison system and in border management.

The workplace is a growing domain as well, with workers using biometrics to access time clocks, cash registers, and secure facilities. Figure 3 shows the spread of different biometric types across these domains. In this type of figure, the length of the box represents the frequency of observations in that category. Fingerprints were the most common biometric in every area except healthcare and education, where iris scanning technology was most prevalent. Interestingly, the technology and financial services domains have embraced the rapid expansion of biometric technology by utilizing all of the available types surveyed.

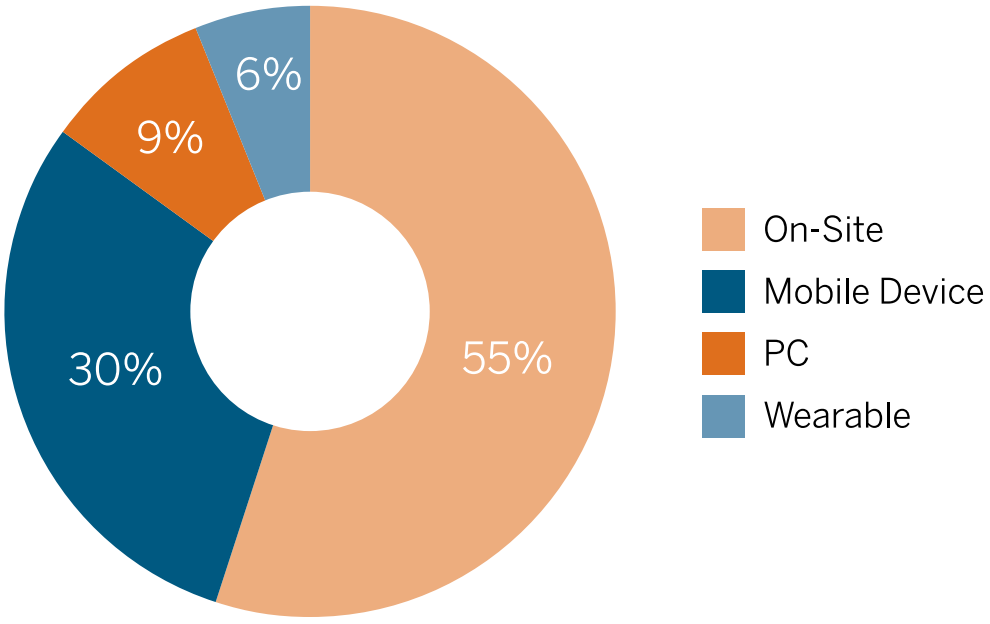
Figure 3.
User Domains and Biometric Types



Platforms

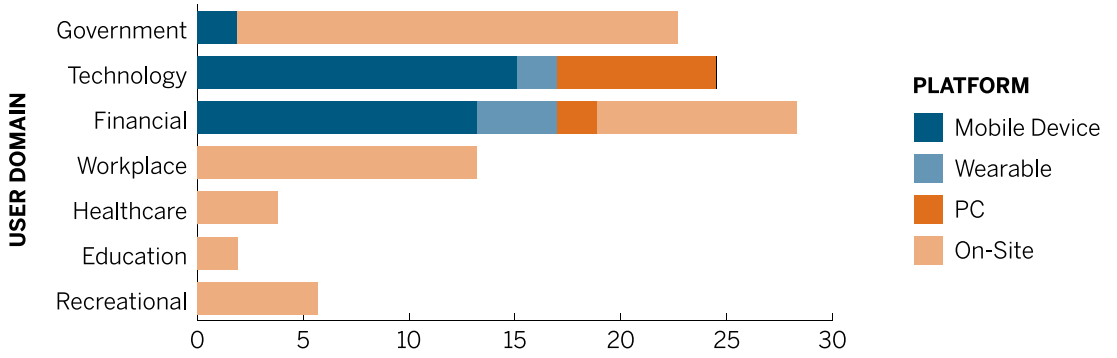
Figure 4 shows variation among the different platforms used to authenticate individuals. Due to the nature of certain services and access privileges, much of the current biometric authentication is performed on-site. From worker identification to in-store purchasing, more and more entities are utilizing the benefits of biometric technology to identify those with access to their systems. But mobile device usage is on the rise, changing the landscape for biometric technology adoption. One example is Samsung's Galaxy Tab, fitted with iris recognition technology for device access as well as banking, education, and healthcare.

Figure 4.
Platforms



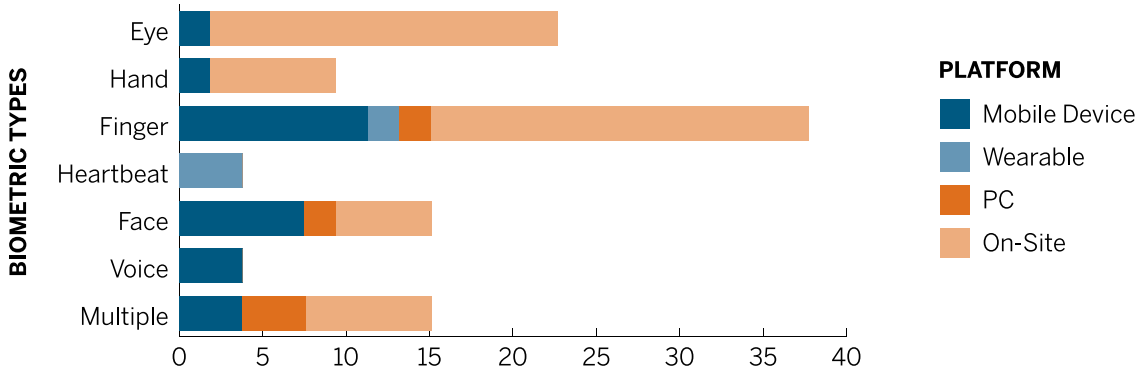
While people are using biometrics across a greater variety of platforms in the areas of finance and technology (e.g. mobile devices, wearables, laptops), on-site usage is prevalent across all settings. Figure 5 shows variation in platform type in each of the seven user domains identified. UCSD's Moore Cancer Center uses iris scanning to uniquely identify their users, while University of Maine implemented palm vein scanners to authenticate students at on-campus dining halls. In healthcare, education, recreation, and the workplace, a growing number of companies are turning to biometrics for identifying their users.

Figure 5.
User Domain by Platform



The types of biometrics used to authenticate users also varies widely by platform. On-site services are the most prevalent, with a wide array of characteristics used. Mobile devices are a close second, though, with a spread across nearly all of the biometric authentication types we looked at. Some PCs and laptops are also being released with biometric capabilities; for example, Clevo has a line of notebooks that use an integrated fingerprint sensor for user access. An emerging market is 'wearables,' such as the Nymi bracelet which measures your heartbeat to authenticate you for your Mastercard on-site purchases. Figure 6 shows variation across plat-forms for each of the biometric types surveyed.

Figure 6.
Biometric Type by Platform



Targeted Activities

Marketers and innovators are rolling out new ways to use biometrics at an accelerating pace. Figure 7 shows the various activities targeted for biometric authentication. Security for personal devices is the most common use for biometrics among the applications surveyed. iProov's Verifier app, available on both Apple and Android devices, allows users to authenticate and unlock their devices via facial recognition. Forecasting for diffusion of biometric enabled smartphones suggest that consumers will have increasing opportunities to use biometrics with their personal devices. But biometric applications in workplace identification, financial sector authentication, and government services are also on the rise. In addition, healthcare providers and recreational facilities such as Disneyworld and Six Flags Arlington use biometric technology to track individual customers throughout their systems and properties. An important distinction here is choice; consumers in some areas such as financial services or recreational activities have the option to provide biometrics or choose another service. Where government and the workplace is concerned, providing biometric data is often a prerequisite for receiving benefits or a mandatory condition of employment.

Figure 7.
Targeted Activities

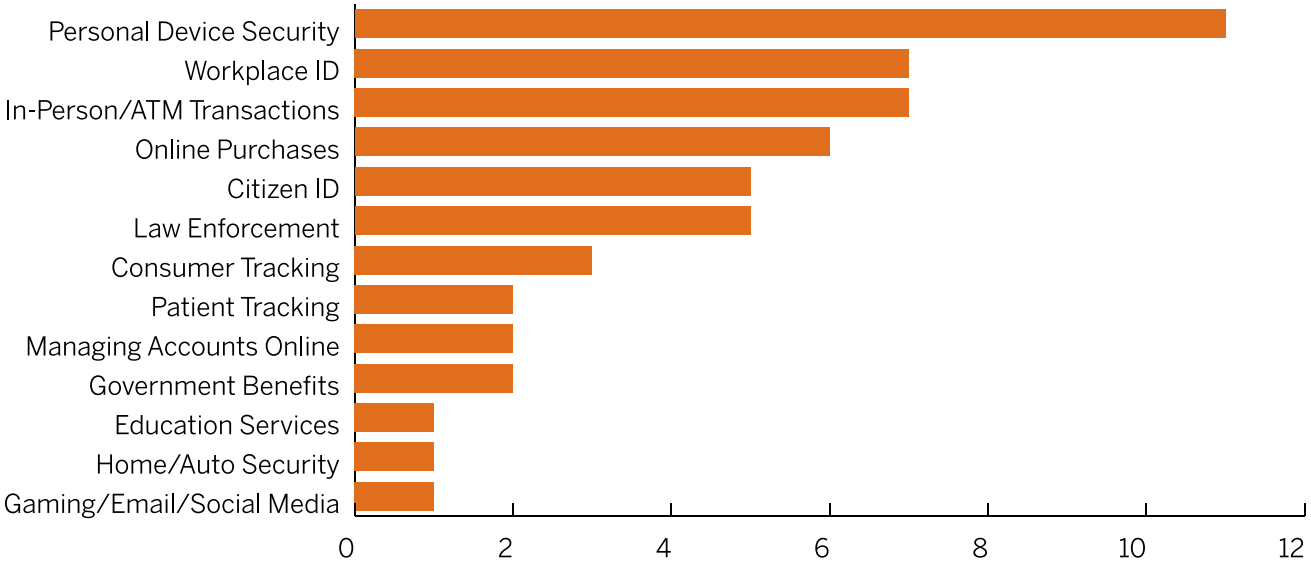
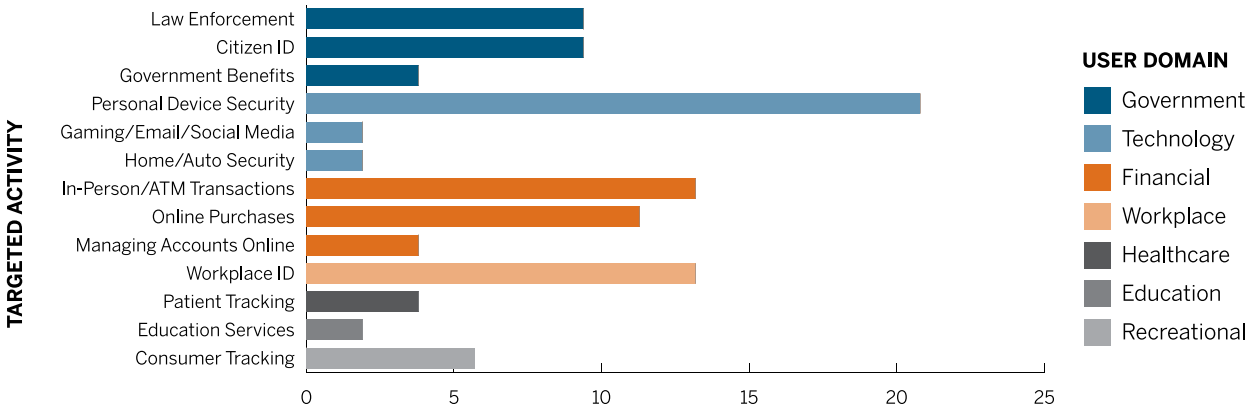


Figure 8 is a breakdown of the targeted activities within each user domain. Governments primarily use biometrics for law enforcement and identifying citizens for services. Personal technology manufacturers have integrated biometrics into many of their products which allows consumers access to devices, property, and internet sites. In the financial domain, online purchases, ATM transactions, and managing accounts and investments are the areas of greatest prevalence for biometrics. Finally, employers increasingly use biometric solutions for tracking and identifying workers.

Figure 8.
Targeted Activities in User Domains



Market Sector

The range of market sectors rolling out biometric authentication solutions is shown in Figure 9. At 19%, information technology is the largest sector integrating biometric authentication into its products and services represented in our survey. Apple was the first company to launch fingerprint recognition technology in smartphones, now standard in many other mobile devices such as Samsung, Motorola, HTC and others. Fujitsu is one of the pioneers in the consumer market, providing laptops and notebooks equipped with PalmSecure, a hand geometry biometrics reader. But plenty of activity is taking place in other industries, the next three - government, finance, and retail - taking up 40% of the remaining applications explored here.

Figure 9.
Biometrics by Market Sector

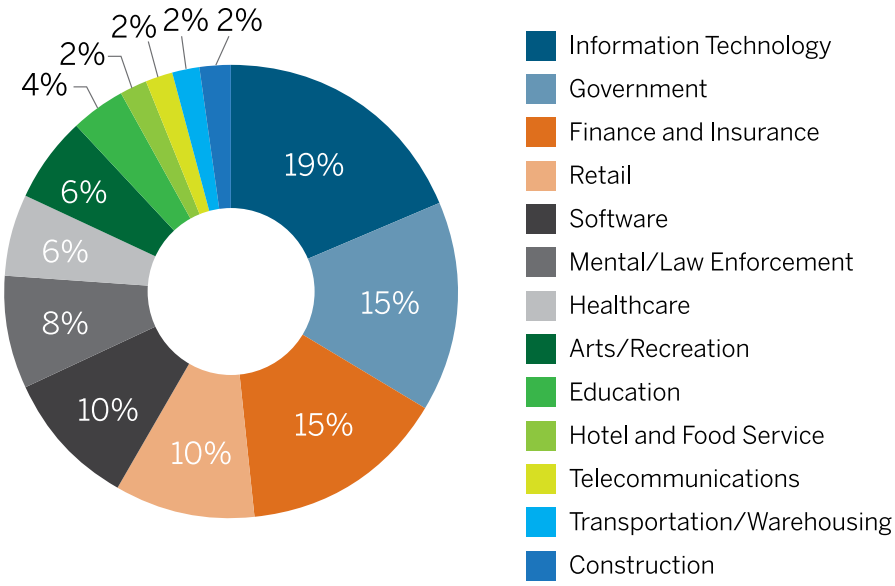
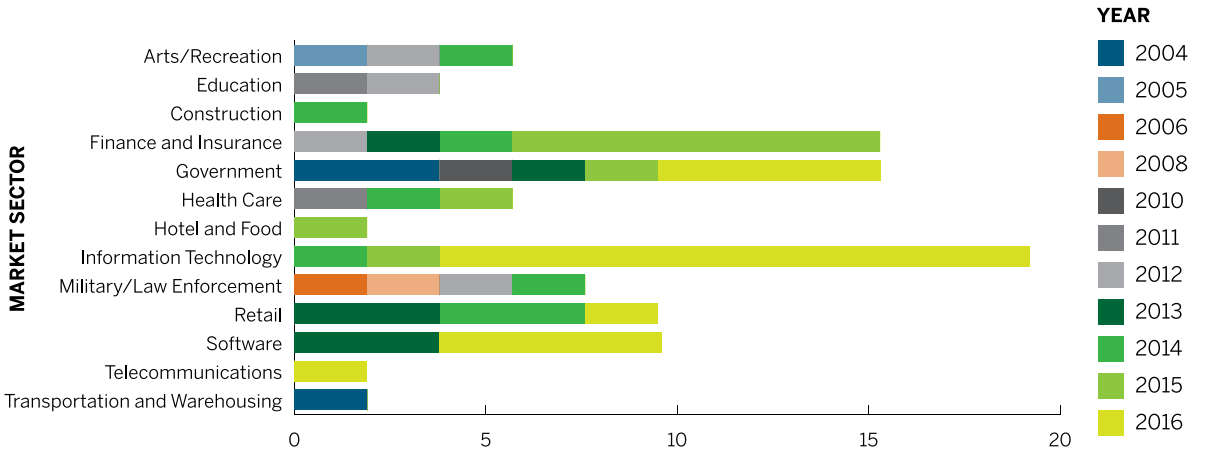


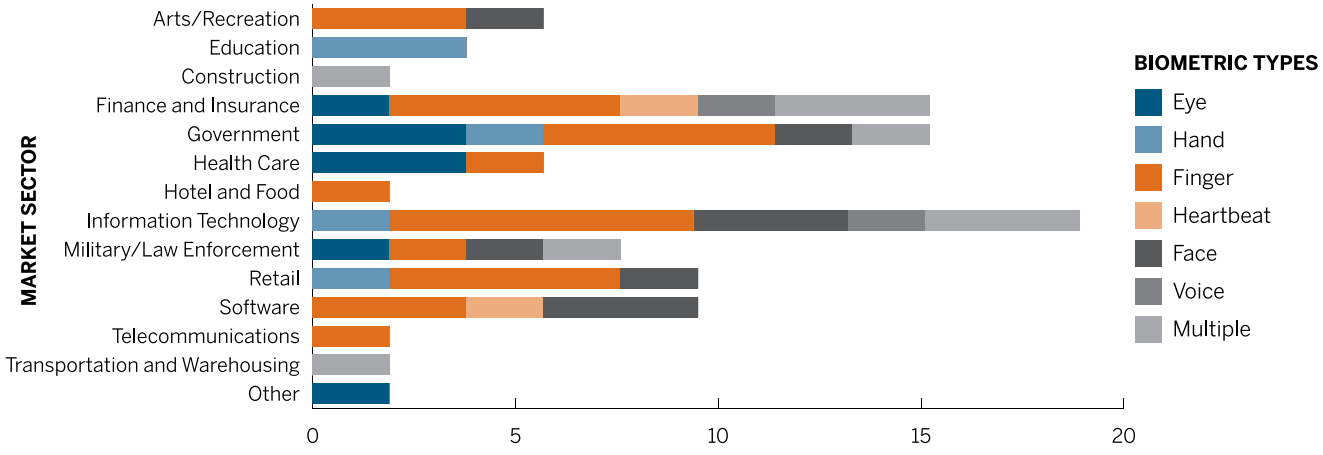
Figure 10 shows biometric trends over the last 12 years in each market sector for all applications in our dataset. While biometric authentication rollouts were mostly limited to government and law enforcement in the beginning of the century, the last five years have seen a rapid increase, not only in adoption, but also in the range of market sectors and targeted consumer activities. In 2012-2016, our data shows an explosive increase in the implementation of new biometric technologies in multiple market sectors, with finance and information technology leading the charge.

Figure 10.
Biometric Market Sector by Year



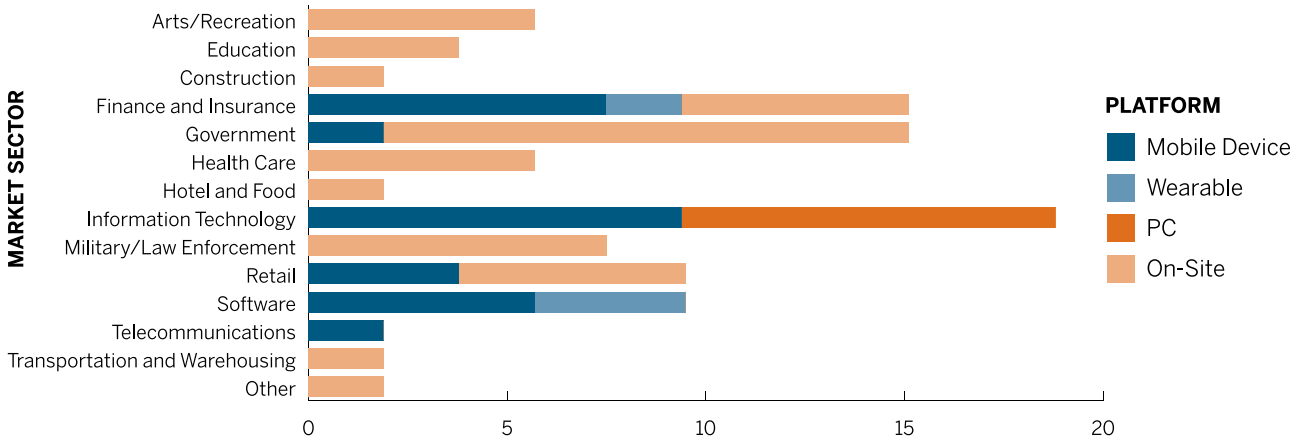
In Figure 11 we can see the range of biometric types used in various market sectors. Fingerprint scanning is the most widely dispersed, with applications in nearly every market sector studied. The use of face recognition technology is increasing in retail, law enforcement and recreation, while iris scanners are being used in government and healthcare. Heartbeat sensors are the least prevalent, but the popularity of Fitbit and the convenience of wearing the sensor suggests an expanding market. Voice recognition is used less often as it is less reliable; when it is utilized it is usually for non-transactional access or as one of multiple factors.

Figure 11.
Market Sectors and Biometric Types



The different platforms used to authenticate users in various market sectors is displayed in Figure 12. Most biometrics are used on site or with mobile devices, however the financial sector and software vendors are beginning to release more wearable biometric scanners, such as the previously mentioned Nymi bracelet and Mastercard credit cards embedded with fingerprint readers.

Figure 12.
Platform Variation by Market Sector



Conclusion

The rapid expansion of biometric technologies has led to a similar explosion in biometric services and applications. Fingerprint scanners are still most common, with face recognition and iris scanners not far behind. The majority of uses of biometric authentication are performed on-site, but mobile device usage is a fast growing area as well. Information technology, finance, and government are the market sectors rolling out most of the publicized application of biometrics for identifying users, with retail and software services close behind.

The activities targeted by companies employing biometrics vary widely. Most common is personal device security, such as unlocking your smartphone, but many employers are coming on board, using biometrics to identify their employees. The biggest change for consumers is in the financial sector, where fingerprint scanners, voice recognition, iris scanners and even heartbeat monitors can be used to access accounts and make purchases. The emerging market of 'wearables' such as the Fitbit health tracker also suggests expanding possibilities for heartbeat authentication.

While biometric authentication was limited to mostly government and law enforcement in the beginning of this century, the last five years have seen a rapid increase, not only in adoption, but also in the range of market sectors and targeted consumer activities. From the trends identified in this study, we expect adoption of biometric technologies to continue to accelerate and expand across all user domains and market sectors, with financial services, retail, telecommunications, and healthcare leading the charge.

Acknowledgement

The Center for Identity acknowledges and thanks TransUnion for their generous support of this research endeavor.

The Center would also like to recognize Kristin Conklin for her invaluable insight and leadership.

WWW.IDENTITY.UTEXAS.EDU

Peter O'Donnell, Jr. Building • Room 5.402 • Mail Stop C4300 • 201 East 24th Street, Austin, Texas 78712