The University of Texas at Austin
Center for Identity

Consumer Attitudes About Biometric Authentication

Rachel L. German

K. Suzanne Barber

UT CID Report# 18-03

May 2018

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

TransUnion®

Executive Summary

Less than a decade ago, consumers largely viewed biometric applications as clandestine extensions of government and law enforcement. Business initiatives relying on biometric applications once failed across market sectors, for a variety of reasons, but that trend appears to be changing as younger consumer generations are now surrounded by smartphones, selfies, mobile payments, and wearables. The advantages of using biometrics for authentication and verification of identity, such as stability and uniqueness, make it a promising avenue for the marketplace. However, consumers overall have still been slow to embrace the widespread use of biometric technology.

Researchers have cited several reasons for reluctance to use biometric authentication technology, including lack of confidence in their reliability (for organizations) and user apprehension. These user concerns could inhibit the mass acceptance of biometric authentication and lead to lack of trust in business applications utilizing biometrics for authenticating clients and customers. This report presents the findings from a survey of 1000 respondents about their familiarity and comfort with biometric authentication. We examine the trend of consumer biometric acceptance and adoption and analyze the factors affecting consumer comfort with biometrics. Some of the questions we address in this report include:

Do consumers use biometrics for accessing their accounts and devices? Yes. More than 42% of participants use biometrics for unlocking their personal devices, usually fingerprint recognition. The most popular account use for biometrics is financial services, with 17% using them to access personal banking, and 5% to manage investments online.

Do consumers realize when they are giving biometric data to an organization? A significant proportion of those using biometrics appear to not have recognized them as such at the beginning of the questionnaire. Alternately, they might not consider 'giving' the information to their phone the same thing as giving it to the organization.

Which type of biometrics are consumers most comfortable providing? Of all biometric types included in the survey, participants were most comfortable giving their fingerprint in biometric form, with 58% saying they were very comfortable, and 28% saying they were somewhat comfortable.

Are consumers concerned about the misuse of their personal information? 42% of participants say they are very concerned about the misuse of their personal information, and 44% are somewhat concerned.

Key Findings

Organization: In this section, we provide a deeper analysis of the findings. Descriptions of the demographics of participants in this research can be found in the appendix of this report. We have organized this report according to the following topics:

1. General Biometric Use and Comfort
2. Understanding Biometrics
3. Comfort and Context
4. Policy, Privacy and the Future

Appendix

1. Demographics

KEY FINDINGS: PART I

Biometric Use and Comfort

The vast majority of respondents have personally experienced fingerprint recognition biometrics, with most saying they have experienced fingerprint scans.

Figure 1 Shows the totals for whether participants have ever provided identifying characteristics to an organization for a computer-matched biometric comparison. The majority, 58%, says they have not, while 36% say they have. They were then asked what types of biometrics they had used previously. Survey participants were asked to indicate all types of biometrics they had personally experienced, and could select multiple types. As shown in Figure 2, 70% of survey participants said they had used a biometric fingerprint scan; this was by far the most commonly selected response.

Figure 1. Provided Identifying Characteristics to an Organization for Biometric Comparison

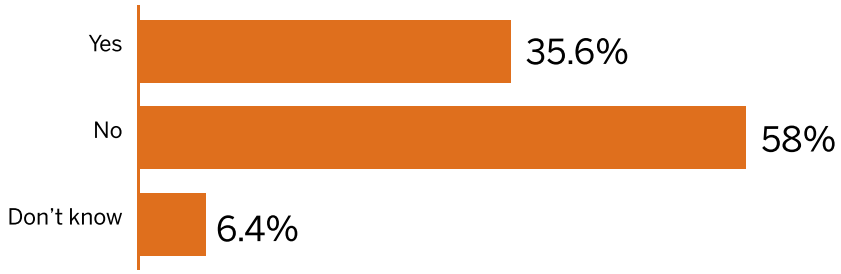
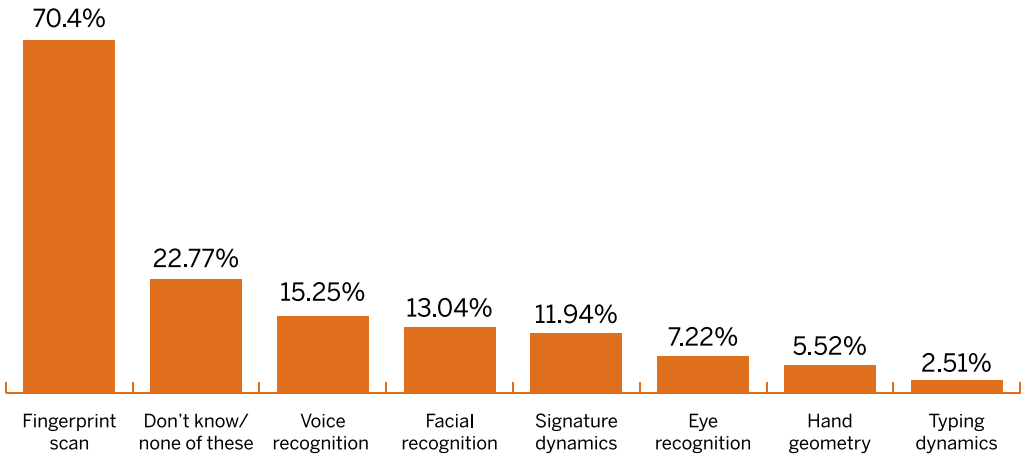


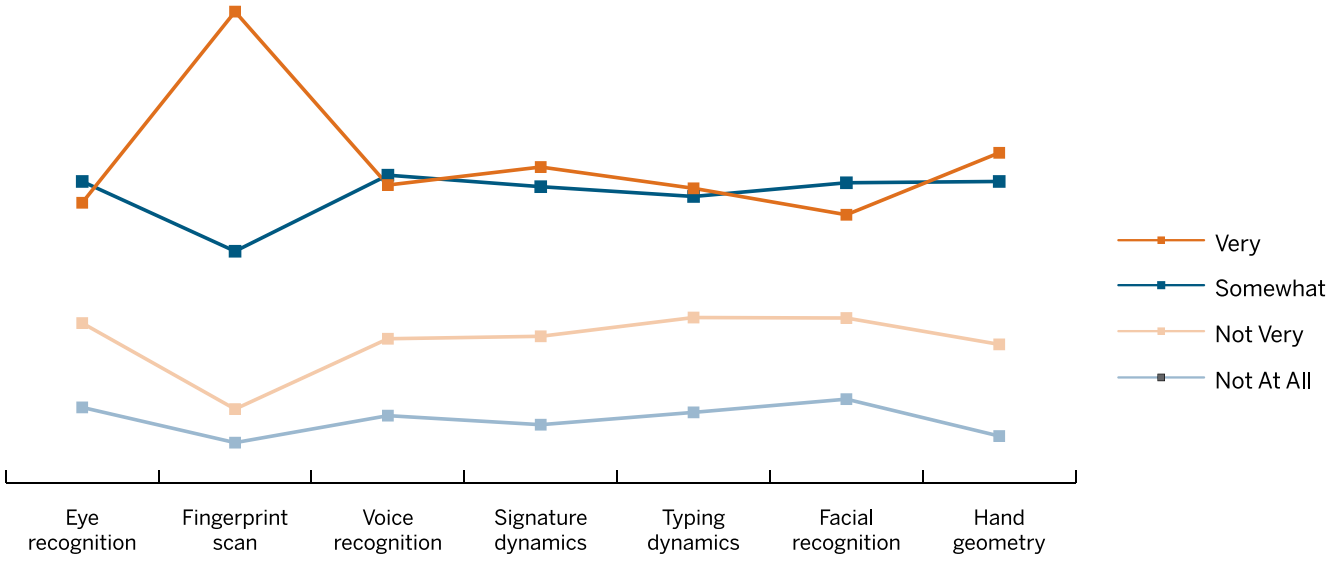
Figure 2. Types of Biometrics Used



Most respondents were comfortable with biometrics, particularly fingerprint scans.

Figure 3 shows the trend for general comfort with different types of biometrics. There is not much variation among most types, with the exception of fingerprint scans. 58% of respondents said they were very comfortable with using fingerprint recognition biometrics, compared to from 33-40% for other types. However, from 68%-76% of respondents said they were either very comfortable or somewhat comfortable with each of the biometric types. Figure 4 shows how comfortable respondents felt each biometric type according to their general comfort with providing them.

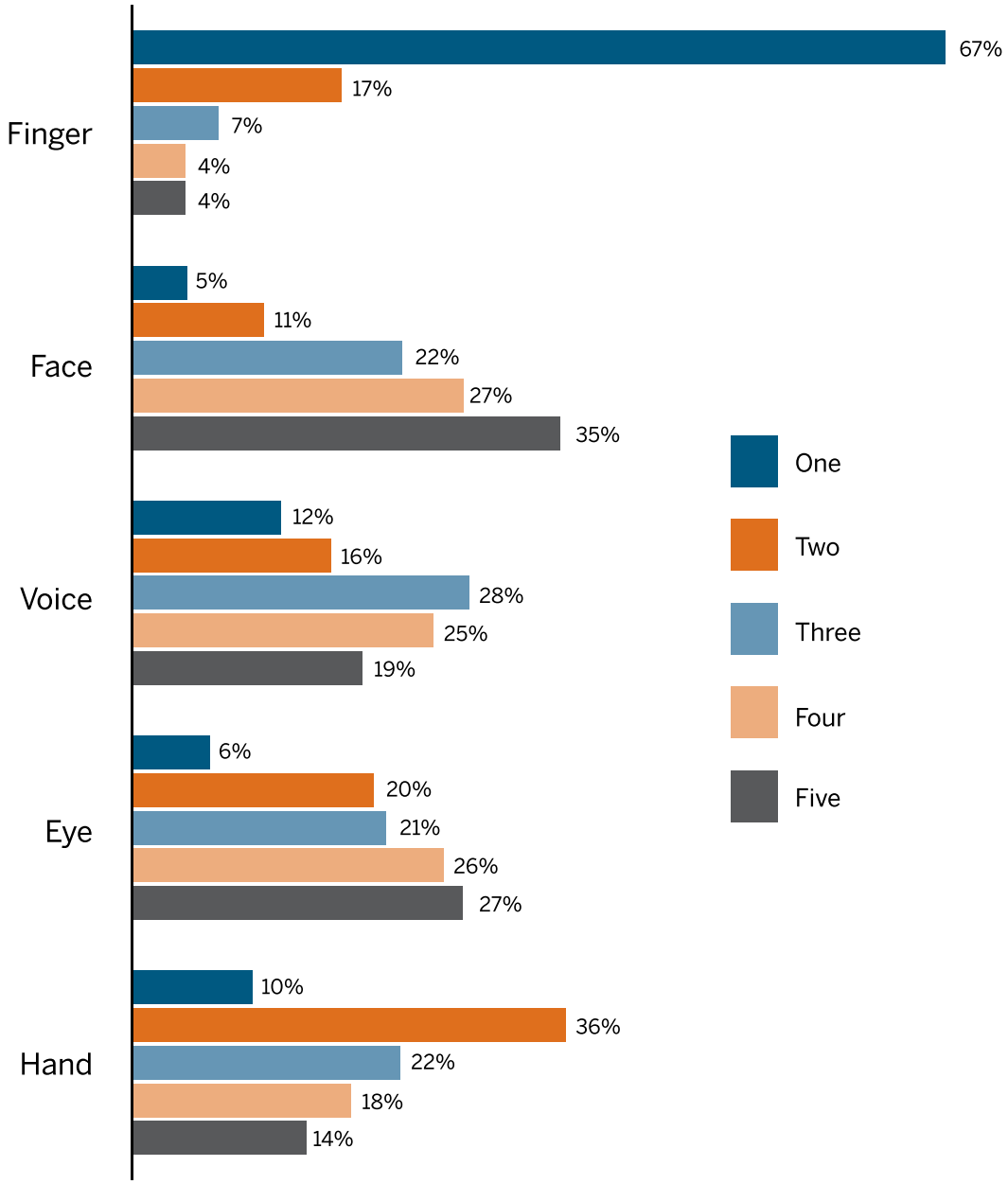
Figure 3. Provided Identifying Characteristics to an Organization for Biometric Comparison



Respondents more often ranked fingerprint as the method they were most comfortable with and face recognition the least.

67% of participants ranked fingerprint as the most comfortable, while 35% ranked facial recognition as the least. This could be influenced by the ubiquity of fingerprint biometric technology in smartphones or other devices, as well as negative media coverage relating to the use of facial recognition software for tracking and surveillance purposes.

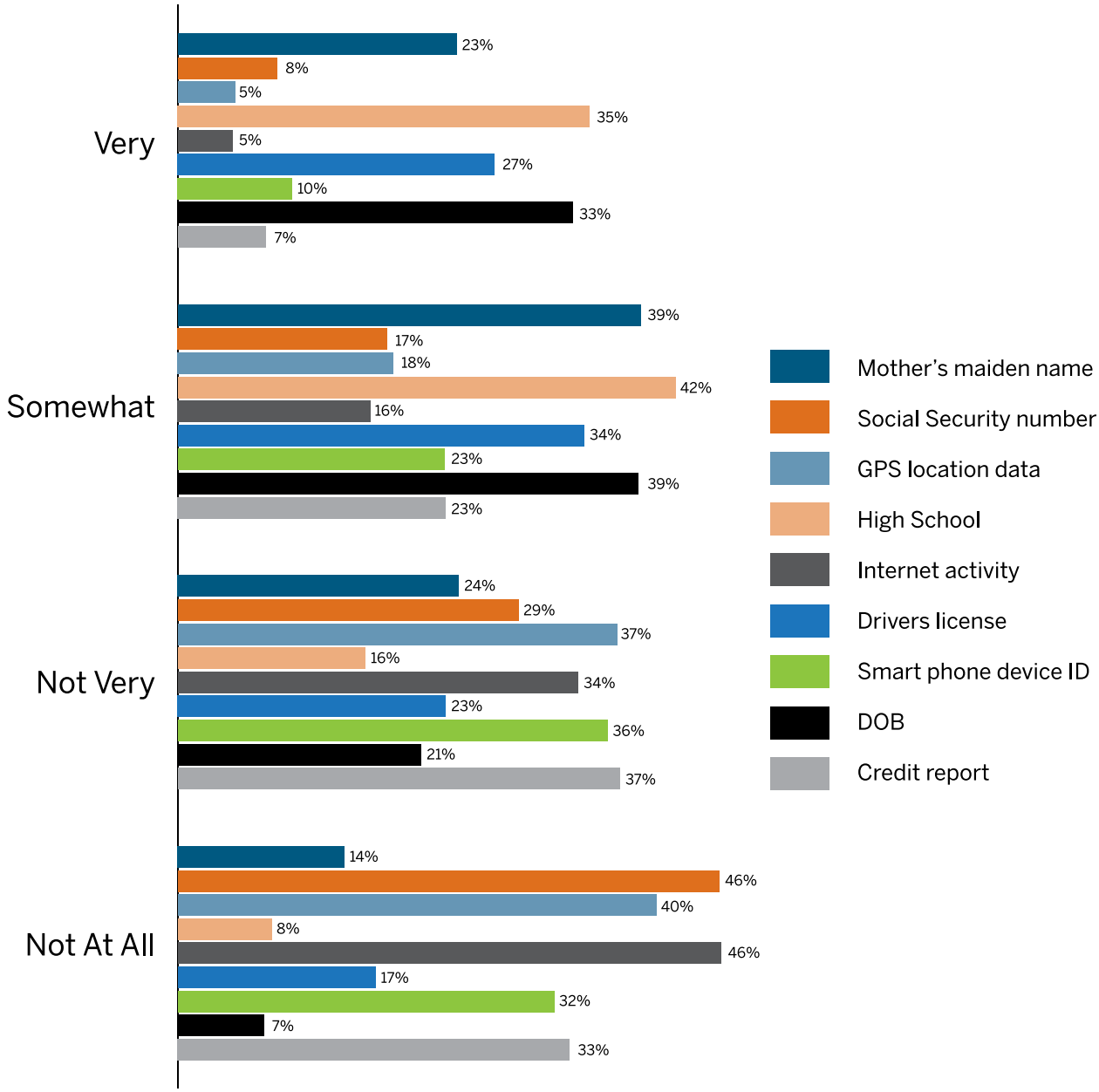
Figure 4. Biometric Type Comfort Ranking from 1 to 5



There is wide variation in general comfort with providing other types of typically collected personally identifiable information for authentication of identity.

Figure 5 shows comfort with traditional forms of PII. 77% of respondents were very or somewhat comfortable with entities collecting information about their high school, 72% their date of birth, and 62% their mother's maiden name. However, from 70% to 80% of participants reported feeling not very or not at all comfortable with providing their internet activity, GPS information, social security number, smart phone device id, and credit report.

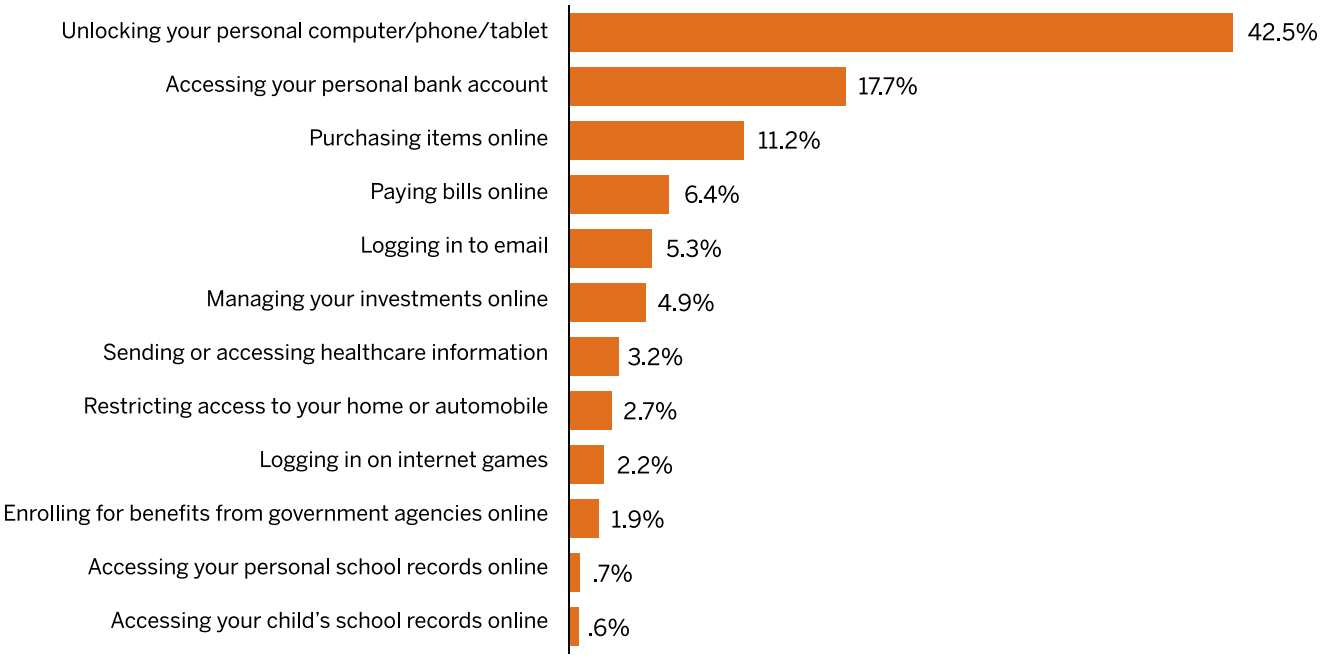
Figure 5. Comfort with Traditional Forms of PII



Many people are already using biometrics for unlocking their personal devices.

Figure 6 shows the number of respondents who say they currently use biometrics for activities such as unlocking their devices, restricting access to other personal items, and accessing their personal accounts. Over 42% of respondent use biometrics to unlock their personal computer/phone/tablet, nearly 18% for their personal online bank account, and 11% for purchasing items online. Other uses were selected by fewer that 10% of participants.

Figure 6. Current Use of Biometrics for Various Activities



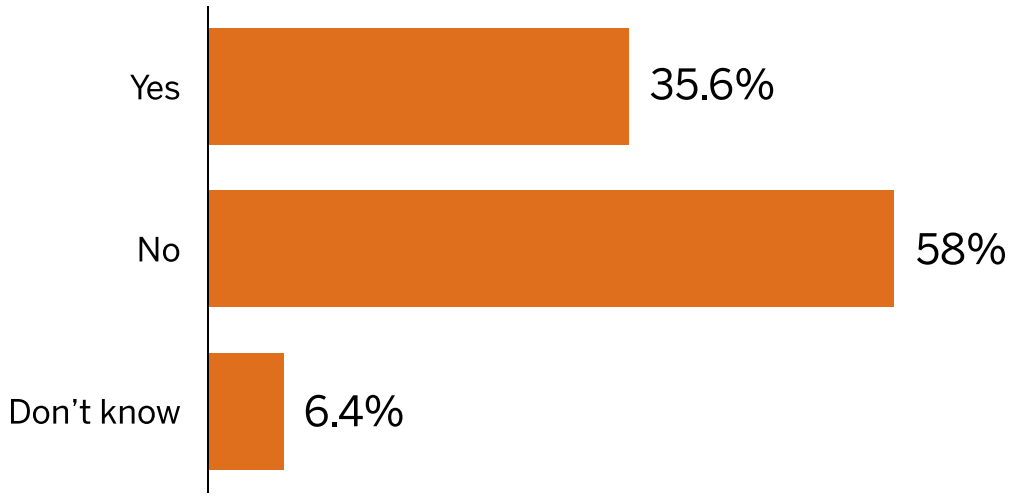
KEY FINDINGS: PART II

Understanding Biometrics

Are People Providing Biometrics to Organizations Without Realizing It?

On the following page, respondents who answered yes, no, or don't know to having experience with biometric authentication are compared with those who said they use biometrics for their personal online activities. When asked "Have you ever personally provided identifying characteristics to an organization for such a computer-matched biometric comparison?" 36% answered yes, while 58% said no, as shown in Figure 7.

Figure 7. Ever Provided Biometrics to an Organization



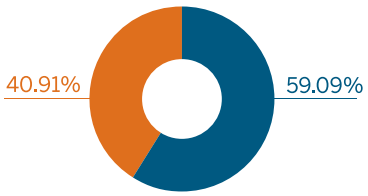
We asked later in the survey if they currently used biometrics for different types of activities.

Figure 8 breaks out the responses to several of the activity responses by whether the participant responded yes or no to the question in Figure 7, "Have you ever personally provided identifying characteristics to an organization for such a computer-matched biometric comparison?" For each person who checked the following apps, the pie graph contains the proportion of those who answered yes/no/don't know to having provided identifying biometric data.

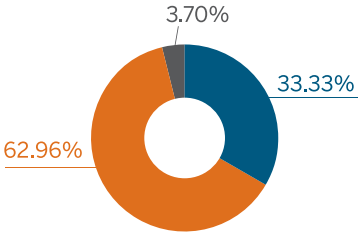
Interestingly, a significant proportion of those using biometrics appear to not have recognized them as such at the beginning of the questionnaire. Alternately, they might not consider 'giving' the information to their phone the same thing as giving it to the organization. From 30% to 71% of respondents who said that they had never provided biometric data to an organization also answered yes to a question about whether they currently use biometrics for activities such as accessing school records, accessing financial accounts, and logging in to email.

Figure 8. Uses Biometrics for Activity by Response to Providing Biometrics to Organization

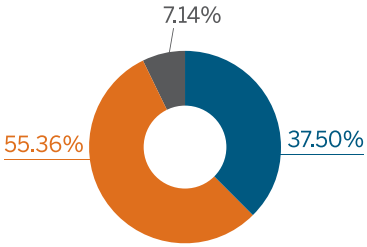
Logging in on Internet games



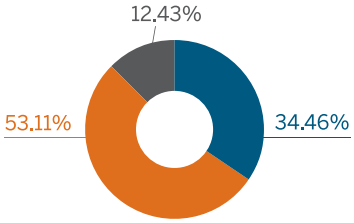
Restricting access to your home or automobile



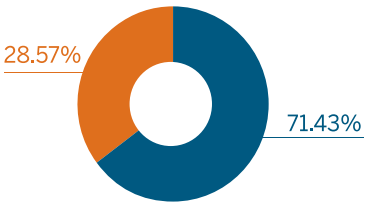
Purchasing items online



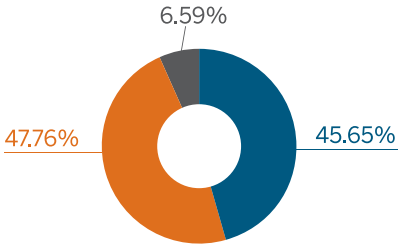
Accessing your personal bank account



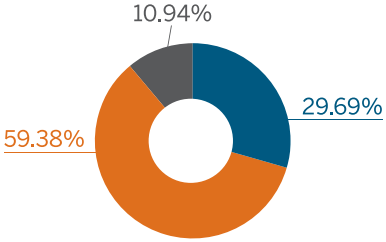
Accessing your personal school records online



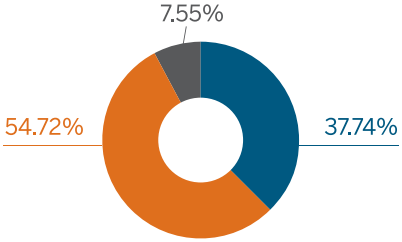
Unlocking your personal computer/phone/tablet



Paying bills online



Logging into email



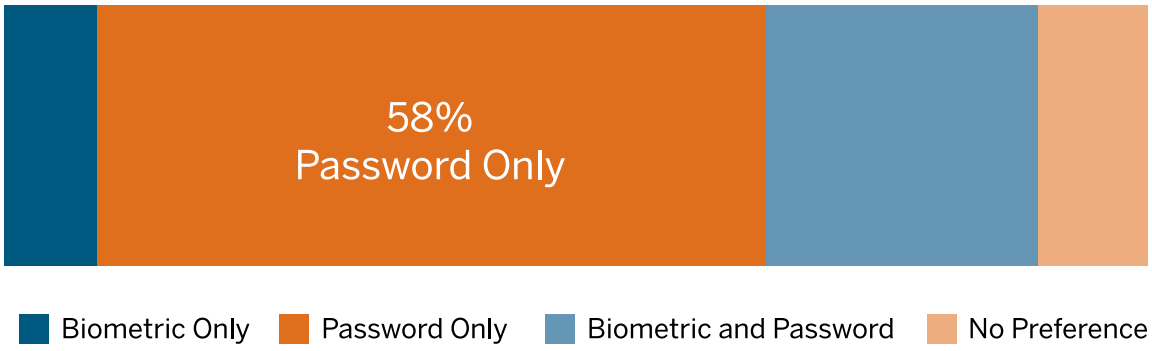
KEY FINDINGS: PART III

Comfort and Context

Most respondents still prefer to use password only rather that a combination of biometrics and password or biometrics alone.

As shown in Figure 9, on average 58% of respondents say they prefer to use only a password to authenticate their identity online. There is, however, some variation in the types of activities for which they prefer to use biometrics alone. 28% were comfortable using biometrics for restricting access to their home or automobile, but fewer than 10% felt the same way about using biometrics alone for activities such as purchasing items online, logging in on internet games, or accessing school records online.

Figure 9. Preference for Password, Biometric, or Both



Invasion of personal privacy is a key concern in providing biometric information.

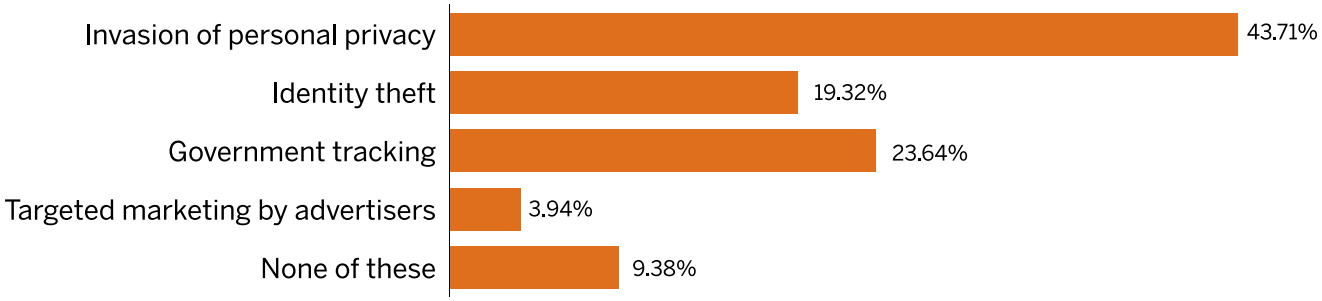
Recall in Section 1 participants were asked to rate their general comfort in providing different types of biometrics. Figure 10 shows the responses.

Figure 10. General Comfort with Biometric Types

	Very comfortable	Somewhat comfortable	Not very comfortable	Not at all comfortable at all
Eye recognition	34.30%	36.91%	19.56%	9.23%
Fingerprint scan	57.72%	28.36%	9.02%	4.91%
Voice recognition	36.47%	37.68%	17.64%	8.22%
Signature dynamics	38.68%	36.27%	17.94%	7.11%
Typing dynamics	36.07%	35.07%	20.24%	8.62%
Facial recognition	32.83%	36.75%	20.18%	10.24%
Hand geometry	40.42%	36.91%	16.95%	5.72%

For each respondent who answered either not very comfortable or not at all comfortable, we asked them to pick one option that best describes their discomfort. Figure 11 show the breakdown of those responses. 43% selected invasion of personal privacy as the reason for their discomfort, while 24% said government tracking. Nearly 20% were concerned about identity theft, but only 4% were most concerned about targeted marketing by advertisers.

Figure 11. Reason for Discomfort



Regardless of private sector or law enforcement context, participants were more comfortable providing their biometric data in person than over the internet

Figures 12 and 13 show responses to the question, "Which of the following methods do you feel more comfortable with collecting your biometric data?" for both law enforcement and the private sector. There is virtually no difference between the responses, with an overwhelming majority preferring in person collection of biometric data.

Figure 12. Preferred Collection Method by Law Enforcement

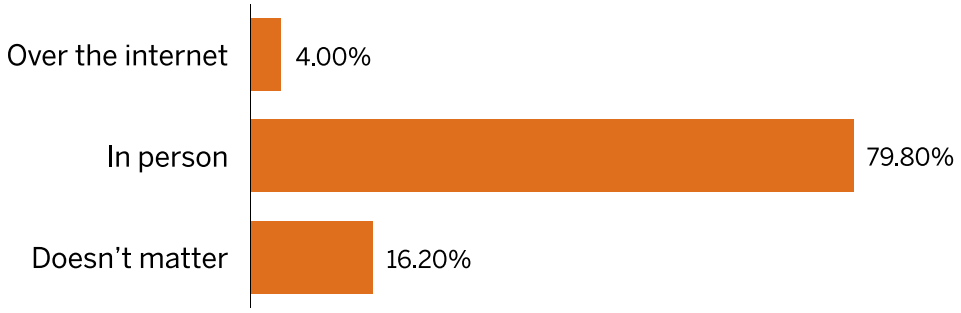
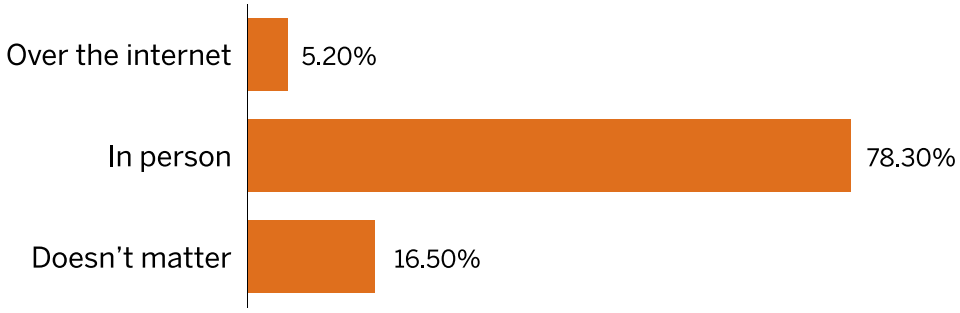


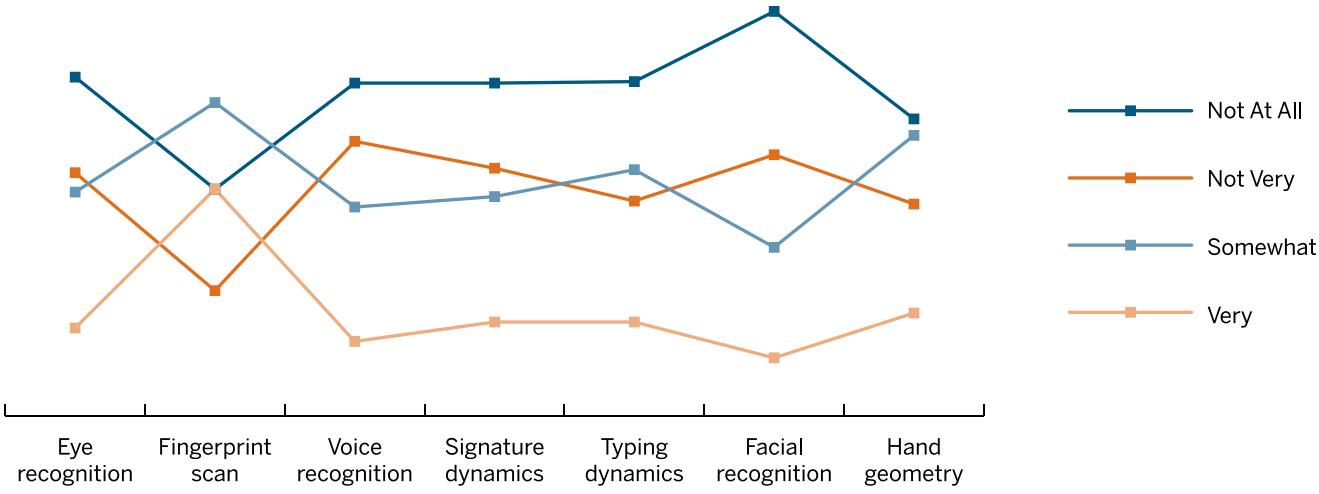
Figure 13. Preferred Collection Method by Private Sector



Context matters more with regard to children under 18 than for elderly relatives.

When asked how they would rate their general comfort with their minor child providing biometric information, responses varied widely according to both the type of biometric and the type of entity collecting it. Figure 14 shows that while a majority said that they are not very comfortable or not comfortable at all with collection of most types of biometrics, the trend reverses for fingerprint scans, with 56% saying they were comfortable or somewhat comfortable. An equal proportion of people, 25%, say they are very comfortable as those who say they are not comfortable at all with their child under 18 providing fingerprint biometrics to the private sector.

Figure 14. Comfort Providing Biometrics in the Private Sector for Child Under 18



Interestingly, reports of comfort for self and for elderly family members were quite similar.

Figures 15 and 16 show comfort with providing biometrics in the private sector for self and for an elderly family member. The major differences in comfort levels for themselves and their elderly family members was that a greater proportion of participants responded that they were somewhat comfortable, rather than very comfortable, with their elderly family members providing biometric data.

Figure 15. Comfort Providing Biometrics in the Private Sector for Self

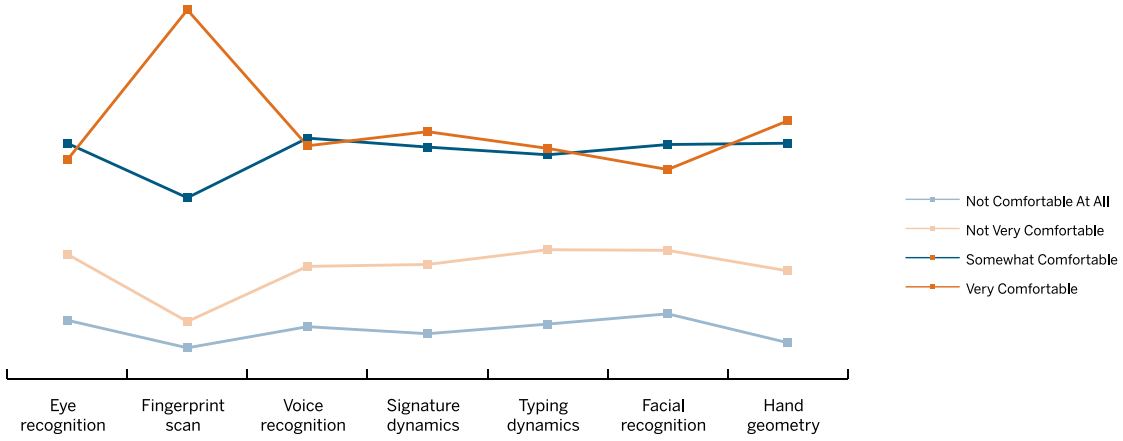
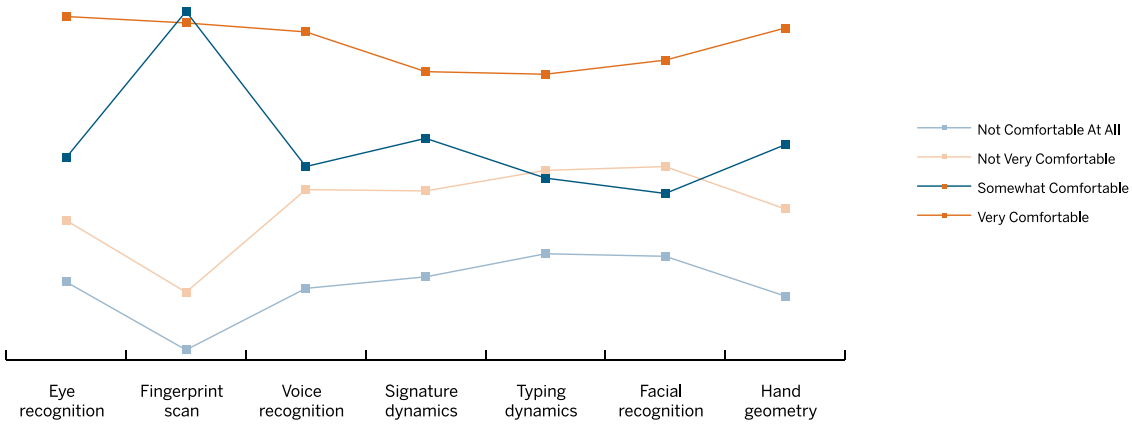


Figure 16. Comfort Providing Biometrics in the Private Sector for Elderly Family Member



Participants are much more comfortable with their elderly family member providing biometrics to law enforcement that they are with their children under 18.

Figures 17 and 18 show comfort with providing biometrics to law enforcement for children under 18 and for an elderly family member. We can see major differences in the comfort levels for children and elderly family members, with the majority not comfortable at all for children and very or somewhat comfortable for elderly family members. An equal proportion of people, 22%, say they are very comfortable, somewhat comfortable, and not comfortable at all with their child under 18 providing fingerprint biometrics to the law enforcement.

Figure 17. Comfort Providing Biometrics to Law Enforcement for Child Under 18

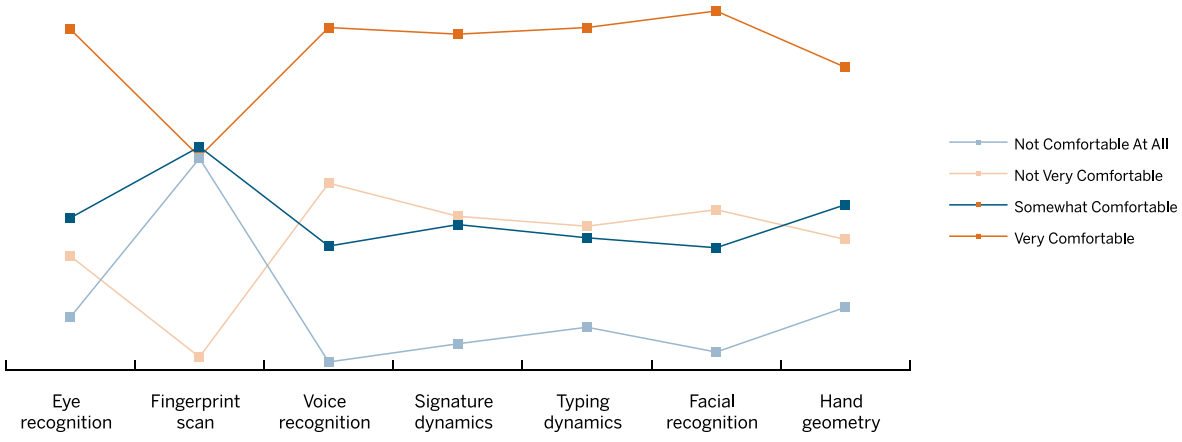
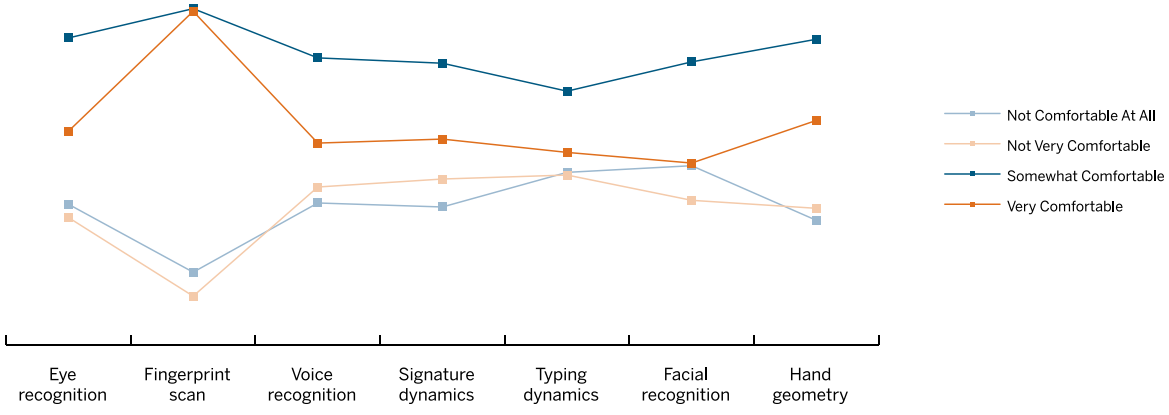


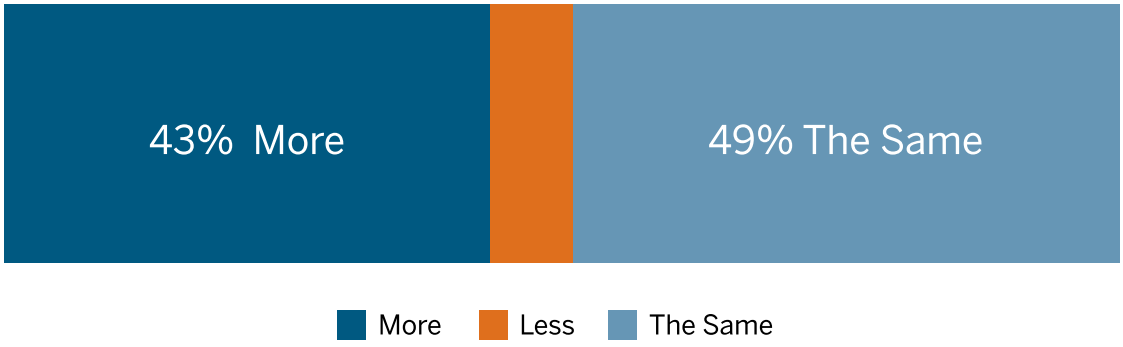
Figure 18. Comfort Providing Biometrics to Law Enforcement for Elderly Family Member



Most people were just as comfortable or more comfortable using biometrics to access devices or accounts today than they were two years ago.

Despite variation across types and contests, most participants reported feeling more comfortable with biometrics today than in the past. In Figure 19 we see that only 8% of respondents say they are less comfortable using biometrics today as compared to two years ago. 49% reported feeling the same, while 43% reported feeling more comfortable using biometrics for accessing devices and accounts.

Figure 19. Comfort Today with Using Biometrics as Compared to Two Years Ago



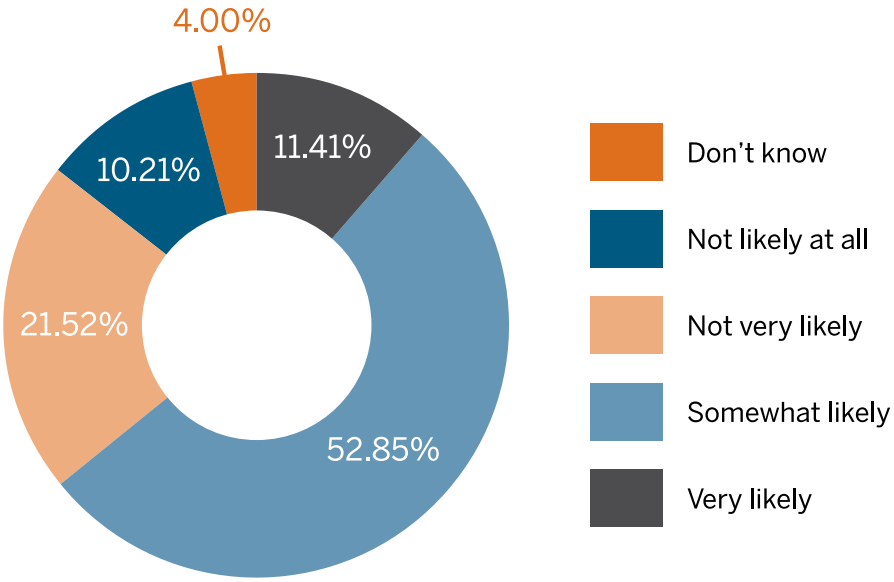
KEY FINDINGS: PART IV

Policy and the Future

Most participants believe it is likely that government will adopt effective safeguards to protect their privacy.

Figure 21 shows responses to the question, "How likely do you think it is that effective safeguards for individuals' privacy will be adopted by government?" 64% of those surveyed believed it was very likely or somewhat likely that effective safeguards would be adopted by government, while 32% thought it was not very likely or not likely at all.

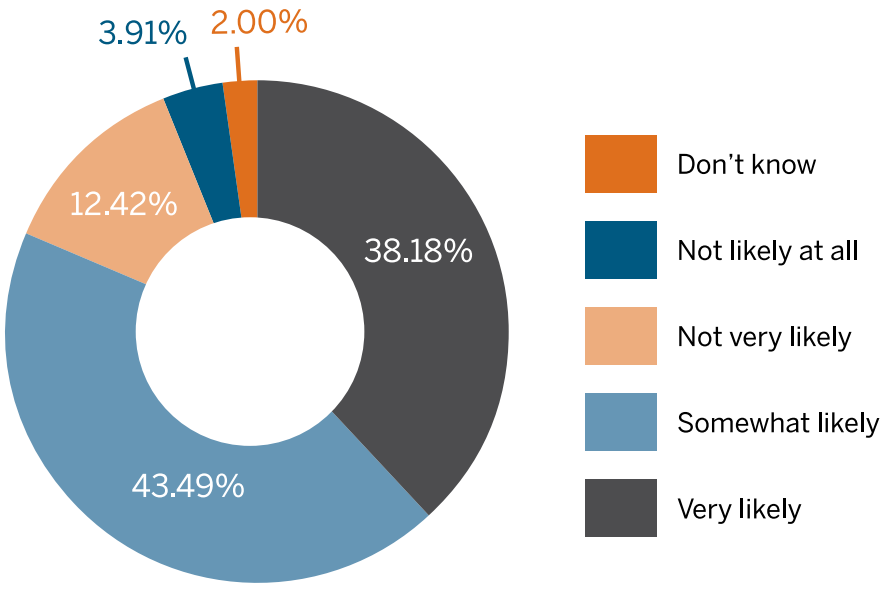
Figure 20. Likelihood of Government Adopting Effective Safeguards for Privacy



Most respondents believe that all adults in the US will have some form of biometric authentication on file by the end of the decade.

Figure 22 shows the responses to the question, "How likely do you think it is that, by the end of this decade, almost every American adult will have at least one biometric ID on file somewhere to verify their identity?" 82% believed it is very likely or somewhat likely, while only 16% thought it was not very likely or not likely at all.

Figure 21. Likelihood of All Adult Americans Having a Biometric ID on File by 2020



Nearly one third of participants have been a victim of invasion of privacy by a business.

Figure 23 shows that 32% of respondent say they have personally been the victim of an improper invasion of privacy by a business, with 56% saying they have not. 12% said they did not know whether or not they had been victims. In Figure 24 we can see that a vast majority, 86%, are either very or somewhat concerned about the misuse of their personal information.

Figure 22. Ever Been a Victim of Invasion of Privacy by a Business

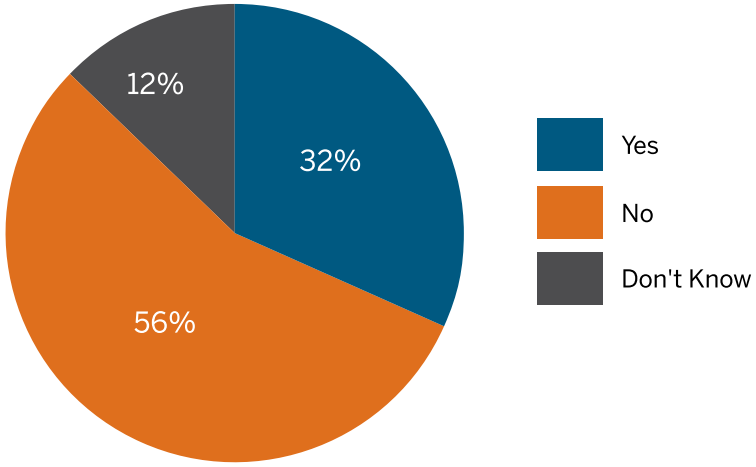
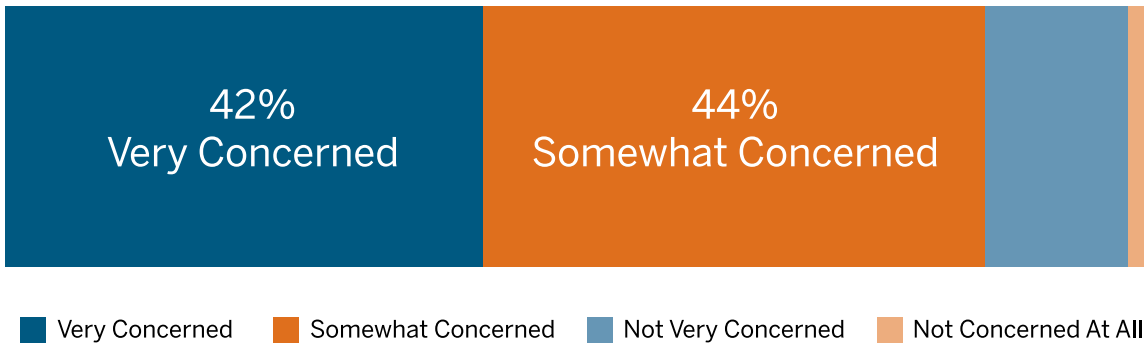


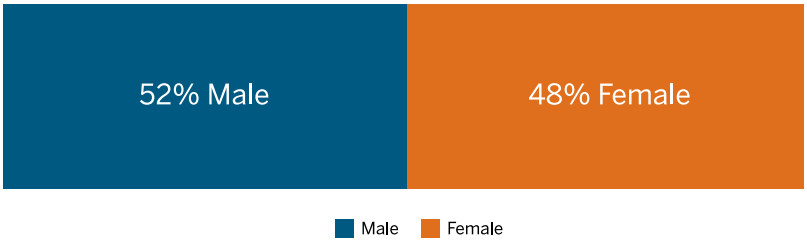
Figure 23. Concerned about Misuse of Personal Information



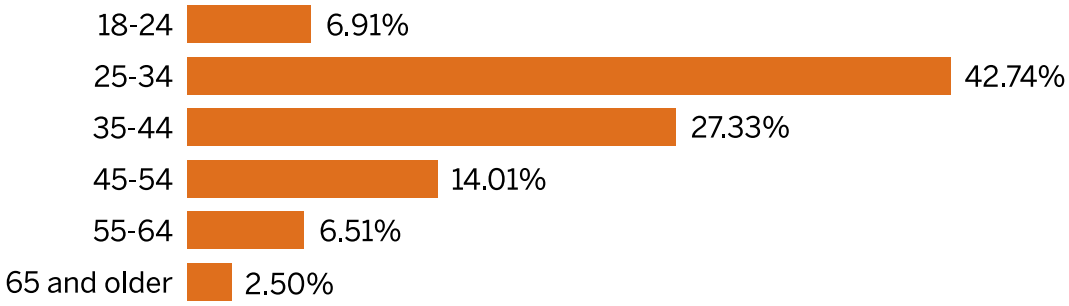
APPENDIX

Demographics Figures

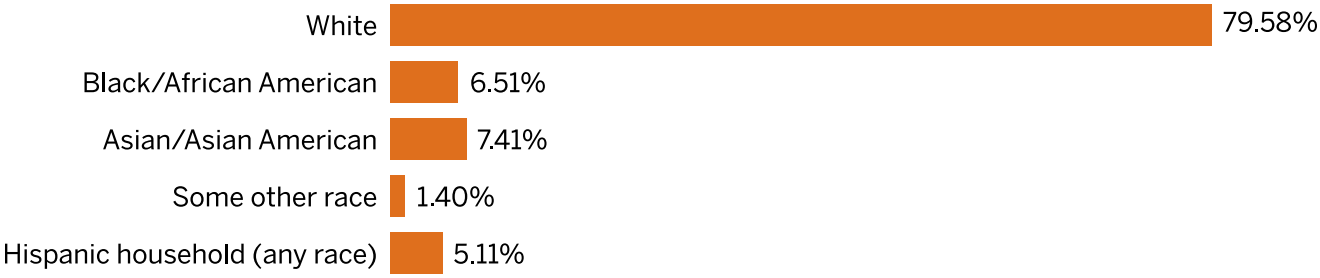
Gender



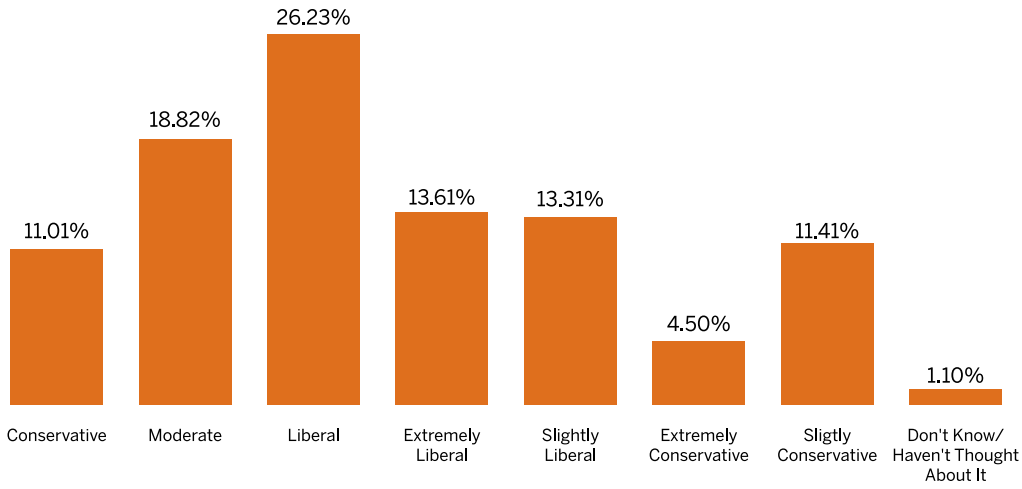
Age



Race/Ethnicity

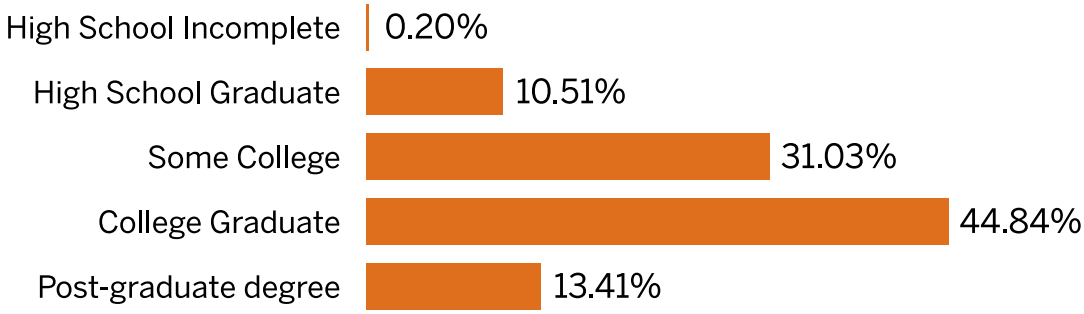


Political Opinion

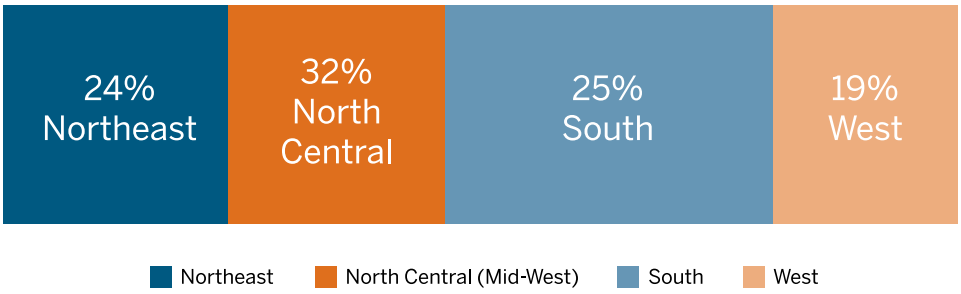


Household Income

Education

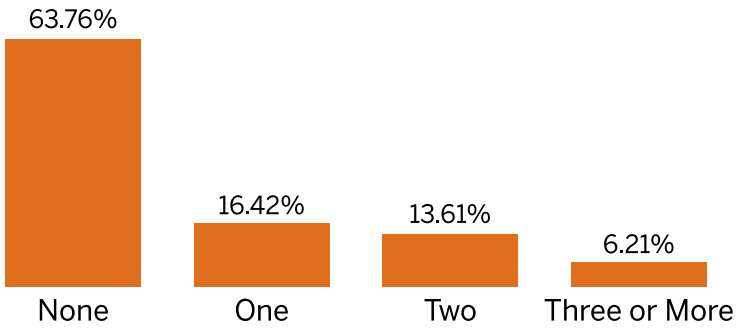


Geographic Region

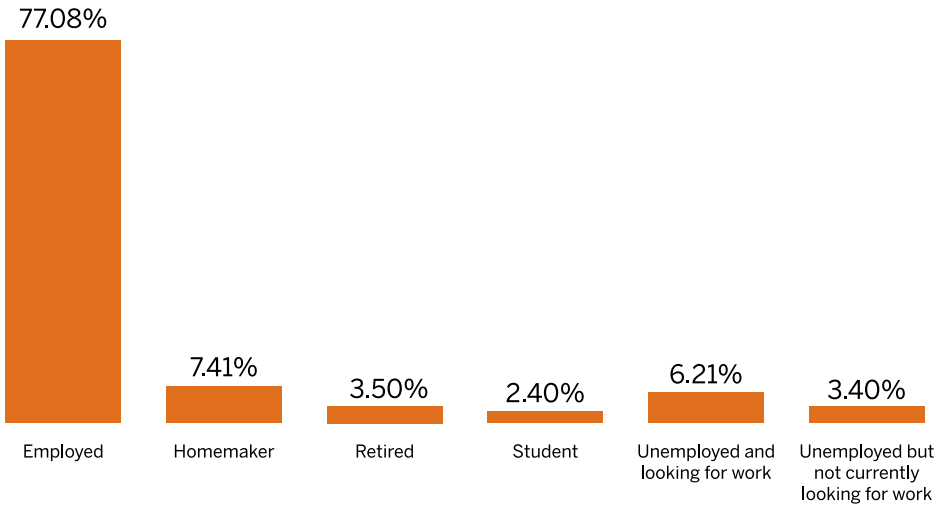


Children:

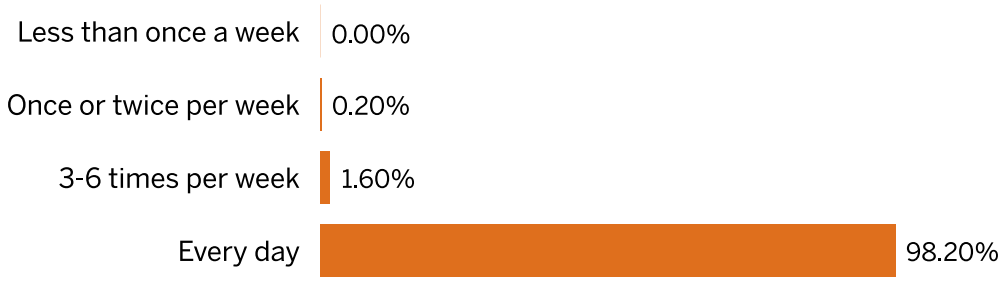
How many children under 18 years old live in your household?



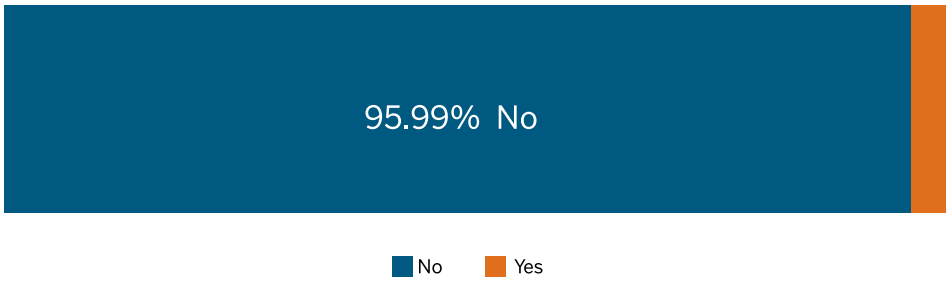
Employment Status



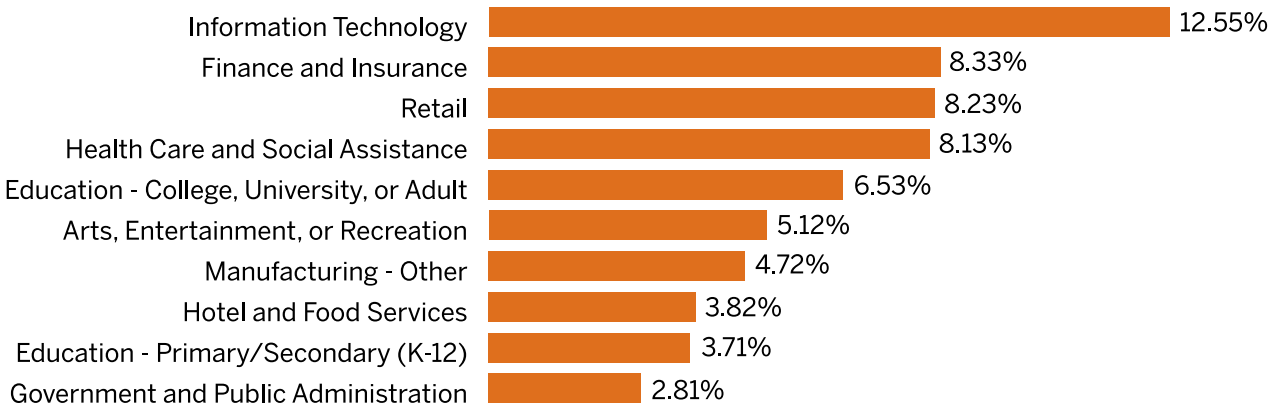
How often do you use the internet?



Military Status:
Are you a current or former member of the US Military?



Industry:
Which of the following categories best describes your primary area of employment?



WWW.IDENTITY.UTEXAS.EDU