Concerns About Online Data Privacy Span Generations

July 2019

Concerns About Online Data Privacy Span Generations

Table of Contents

I. Executive Summary

The Internet Innovation Alliance (IIA) is publishing this white paper to help inform policymakers at all levels about the views of U.S. consumers concerning their online data privacy. To underscore the urgency for Congress to protect Americans by addressing the consumer data privacy issue now with unified, comprehensive legislation, the paper examines privacy abuses, data misuses, and security breaches, and reveals through recent research the indispensable role the internet plays in the lives of Americans.

Additionally, this report outlines the history of privacy regulation in the United States. The Federal Trade Commission's (FTC) longstanding work protecting the privacy of Americans and the impact of actions taken by the Federal Communications Commission (FCC) related to consumer privacy are explained. The accessibility of consumer personal information in the internet ecosystem is also detailed to show the threats to the online privacy of Americans.

New data points are also provided with this white paper, as the result of a comprehensive survey IIA commissioned in April of this year, reflecting the views of more than 8,000 U.S. consumers. The research focuses particularly on the views of a large and important demographic in the United States – Millennial Americans – while at the same time providing important information about the views of other demographic groups including those of Generation X and the Baby Boom Generation. This report also offers information about other demographic segments and consumers of varying income levels. Key findings include the following:

> ***Today's Millennial Americans are deeply concerned about the privacy of their online personal data.*** More specifically, a strong majority of Millennials – two-thirds (67%) – are worried about their personal financial information being hacked from the online/social media companies they use. Nearly three-quarters of Millennials (74%) are concerned about how online tech and social media companies are using their online data and location information for commercial purposes, and more than two-thirds of Millennials (69%) are "not OK" that online tech and social media companies collect and use their personal data in order to make online searches, advertisements, and content more relevant to them. ***Even larger percentages of older Americans – Generation Xers and Baby Boomers – have concerns about their online data privacy;***
>
> ***Concerns about online data privacy breaches are shared by Hispanics, Blacks, and Other Americans, and these concerns stretch across all geographic regions of the United States and income levels.*** For example, strong majorities of Hispanics (68%) and very strong majorities of Blacks (73%) are "not OK" that online tech/social media companies collect and use their personal data to make online searches, advertisements, and content more relevant;
>
> ***A very strong consensus exists among Americans for a single, nationwide online data privacy law.*** The survey shows that support for a single, nationwide online data privacy law is held by Millennials, Generation Xers, and Baby Boomers, as well as Americans of all ethnicities (Whites, Blacks, Hispanics, and those reporting Other) and income levels. Likewise, support for a single, nationwide online data privacy law is strong among Americans living in Rural Areas, Suburbs, and Cities. The majority of Millennials (64%) believe a single, nationwide data privacy law is necessary. ***Overall, 72% of Americans believe there should be a "single, national policy addressing consumer data privacy rules in the United States."***

Based on the findings, IIA calls for the U.S. Congress to recognize that:

- Americans do not trust online tech and social media companies to protect their personal financial information.
- Americans do not want tech/social media companies to collect and use their personal data, even though such practices could make their online searches, advertisements and content more relevant.
- The vast majority of Americans want a single, national policy addressing consumer data privacy in the United States.

Consistent with the views of millions of Americans, IIA believes that policymakers in the U.S. Congress should act on these concerns by crafting a single, nationwide framework for safeguarding the online personal information of U.S. consumers.

II. Consumer Online Privacy in Today's Internet Ecosystem

A. Online Environment & Consumer Online Activities

Millions of Americans are concerned about their online privacy. By some estimates, over 90% of U.S. internet users worry about their privacy online.[1] In its most recent survey of internet use, the U.S. government estimates that nearly "three-quarters of internet-using households had significant concerns about online privacy and security risks," and roughly a third of U.S. consumers scale back their online activity because of their privacy concerns.[2]

And why not? In recent years, consumers have witnessed a steady stream of privacy abuses, data misuses, and security breaches. Some of the high-profile privacy scandals that have bombarded consumers just over the past year include:[3]

- In April 2019, Facebook disclosed that it expects to be fined up to $5 billion by the Federal Trade Commission for privacy violations. This announcement followed recent news that the New York State Attorney General, as well as regulators in Ireland and Canada, are investigating Facebook's consumer data privacy practices.
- In December 2018, Google revealed that a "security bug" affected the personal information of more than 52 million consumers. This followed earlier revelations of similar security issues affecting one of Google's social media platforms.
- In December 2018, Facebook disclosed that a security flaw potentially exposed the personal published and unpublished photographs of nearly 6.8 million users.
- In September 2018, Facebook announced that a security breach exposed the accounts of more than 50 million consumers. This announcement coincided with other reports that Facebook provides advertisers with "shadow contact information," including phone numbers, consumers use for account security purposes.
- In May 2018, reports surfaced that Amazon distributed copies of private, in-home conversations to user acquaintances.
- In May 2018, Twitter advised all 336 million users of its platform to change their passwords following a security breach.
- In March 2018, news outlets reported on the Facebook Cambridge Analytica scandal, which compromised the data of 87 million Facebook users.

And of course, privacy abuses and data breaches occurred in other online contexts, such as hotel chains, department stores, newspapers, banks, restaurants, and credit monitoring services. To take just one example, in September 2018 the Government Accountability Office (GAO) released an in-depth assessment of the Equifax data breach – concluding that this breach alone affected "at least 145.5 million consumers in the U.S."[4] The list could go on. In fact, 2018 appears to be a record year for data breaches and identity theft – ***over 446 million consumer Personally Identifiable Information (PII) records were exposed in 2018,*** primarily through hacking of the business and health care sectors.[5]

1. TRUSTe/NCSA U.S. CONSUMER PRIVACY INDEX 2016.

2. National Telecommunications and Information Administration, Department of Commerce, *Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds* (Aug. 20, 2018) (summarizing online privacy and security findings in survey conducted by the U.S. Census Bureau).

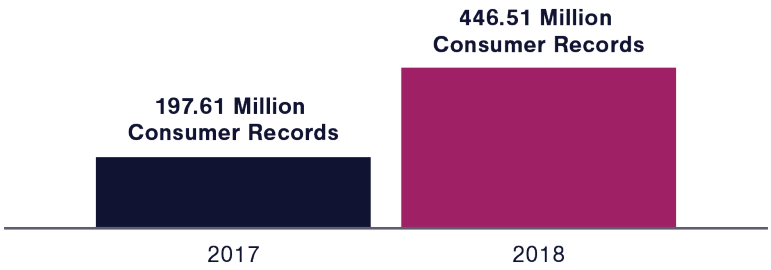
3. Citations to reports from various news outlets are contained in Appendix A.

4. Government Accountability Office, DATA PROTECTION: ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH at 1 (Aug. 2018).

5. Identify Theft Resource Center, 2018 END-OF-YEAR DATA BREACH REPORT (2019).

As demonstrated in the chart below, ***this was a massive increase in the number of consumer records exposed compared to the previous year.*** In its analysis of data breaches in 2018, the Identity Theft Resource Center identified the incidents involving Marriott International, Google, and Facebook as the top three most significant incidents of the year.

Increasing Exposure of Consumer Personal Records



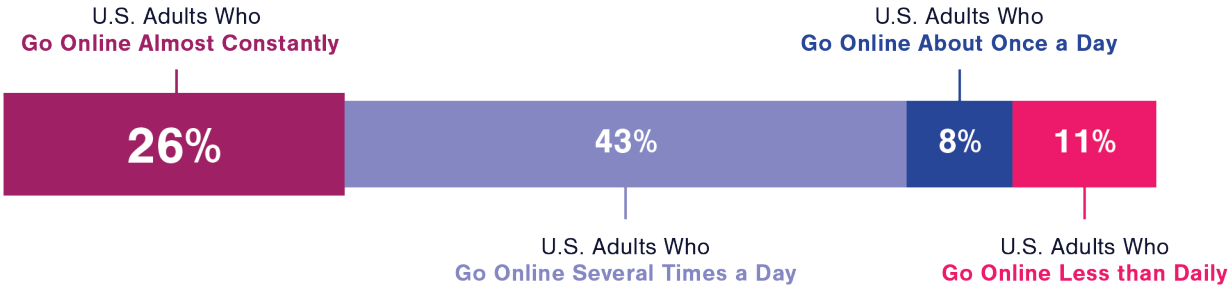
SOURCE: Identity Theft Resource Center, 2018 END-OF-YEAR DATA BREACH REPORT.

Privacy abuses, data breaches, and misuses of personal information continue to dominate the news. While the U.S. government was investigating Facebook for its involvement with Cambridge Analytica, reports surfaced that Facebook collects data from "millions of smartphone users" using apps, "even if no Facebook account is used to log in and if the end user isn't a Facebook member."[6] A number of news outlets have reported on the scope and type of consumer personal information that is made available online to "edge" providers and others.[7] And the federal government issued the record-high fine of $5.7 million against the app provider Muscial.ly (known as TikTok) for misusing and abusing the personal information of children in violation of the Children's Online Privacy Protection Act (COPPA).[8]

Consumer awareness and concern regarding privacy continues to climb as the internet ecosystem expands in importance in the daily lives of U.S. consumers. The internet is a vital resource; it's seen by many as essential. Consumer devices and products are increasingly connected to the internet, and consumers continue to take advantage of a proliferation of new online-based services and applications. As noted in the chart below, about a quarter of U.S. adults report that they are "almost constantly" online, and roughly three-quarters of Americans go online at least daily.

Roughly Three-Quarters of U.S. Adults Go Online At Least Daily

% of U.S. Adults who say they go online ....



SOURCE: Pew Research Center, A*bout A Quarter of U.S. Adults Say They Are "Almost Constantly" Online* (Mar. 14, 2018).

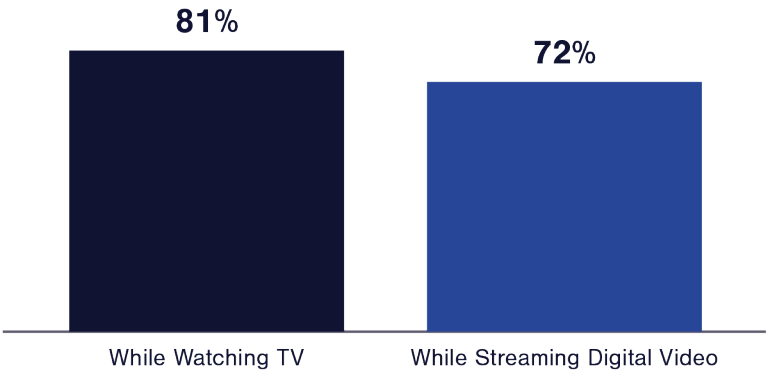
6. The Wall Street Journal, Sam Schechner and Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook* (Feb. 22, 2019); The Wall Street Journal, Sam Schechner, *Eleven Popular Apps That Shared Data with Facebook* (Feb. 24, 2019).

7. The New York Times, Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret* (Dec. 10, 2018); The New York Times, Jennifer Valentino-DeVries, *Uncovering What Your Phone Knows* (Dec. 14, 2018).

8. *See* Federal Trade Commission, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law,* Press Release (Feb. 27, 2019).

And not only has online activity increased, but consumers are also choosing to use multiple devices at one time. As shown in the chart below, most U.S. adults choose to use a "second screen" (either a smartphone or a tablet) while watching television or while streaming digital video. While using a second screen, many consumers shop online, search for news and information, and engage with their family and friends over social media.

Most Consumers Use Second Screens While Watching Video



SOURCE: Statista, SECOND SCREEN USAGE, *Percentage of internet users in the United States who use another device while watching TV or streaming digital video on TV as of March 2017,* pg. 9 (2019).

Consumers now use the internet for daily activities that were barely imagined almost 30 years ago. They rely on the internet and broadband connectivity to communicate with friends and family, upload photos, buy and sell items, research potential purchases, use search engines to find information, read or watch news and sports, make travel arrangements, obtain government services, and more.[9] Just in the area of online commerce, U.S. consumers use the internet to purchase hundreds of billions of dollars worth of goods and services. Over 95% of internet-using U.S. adults report some level of online shopping.[10] In 2017 alone, e-commerce retail sales topped $453 billion.[11] Independent analysts estimate that, in 2018, over 220 million digital shoppers used the internet for shopping and retail e-commerce sales in the U.S., totaling over $504 billion.[12] Consumers also spend a significant amount of time engaged in online shopping – they spend on average more than 14 hours each month shopping online.[13]

9. *See, e.g.,* CivicScience, INTERNET BEHAVIORS AND ATTITUDES PROJECT (Aug. 15, 2017) (presenting survey data to show how U.S. consumers use the internet).

10. Statista, ONLINE SHOPPING BEHAVIOR IN THE UNITED STATES, *Online shopping reach among online users in the United States as of December 2017, by device,* pg. 11 (2019).

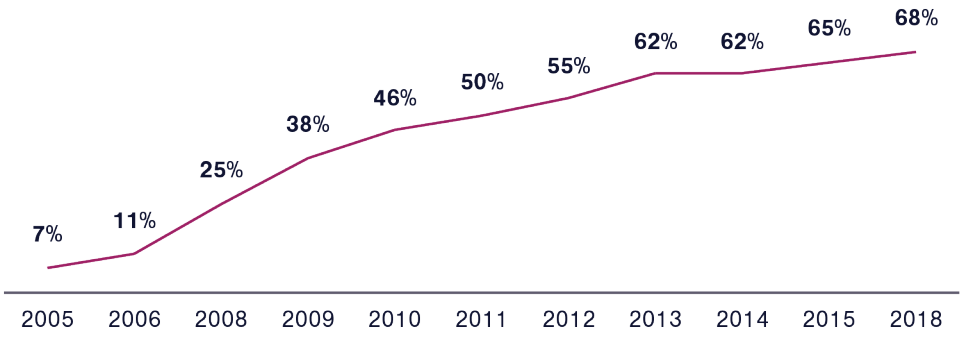
11. Dept. of Commerce, U.S. Census Bureau News, Quarterly Retail E-Commerce Sales (1Q2017 through 4Q2017). The most recent U.S. Census Bureau Quarterly Retail E-Commerce Sales report notes that total U.S. retail e-commerce sales for the 3rd quarter of 2018 were estimated at $130.9 billion, which brings total U.S. retail e-commerce sales for the period January through September 2018 to exceed $380 billion.

12. Statista, *Retail e-commerce sales in the United States from 2017 to 2023* (2019) (reporting U.S. retail e-commerce sales in 2018 to be $504.6 billion, which is approximately a 13% increase over the $446.8 billion reported the prior year).

13. Statista, ONLINE SHOPPING BEHAVIOR IN THE UNITED STATES, *Monthly time spent on online shopping by users in the United States as of December 2017, by shopper type (in minutes),* pg. 48 (2019). In the survey conducted in December 2017, all shoppers reported on average conducting 846 minutes, or about 14.1 hours, in online shopping. Light Shoppers reported spending 72 minutes, or about 1.2 hours; Medium Shoppers reported spending about 411 minutes, or 6.85 hours, in online shopping; and Heavy Shoppers reported spending 2,675 minutes, or about 44.6 hours, shopping online in that month.

U.S. consumers have also flocked to social media platforms in the past decade, and surveys confirm that social media now plays a leading role in the daily lives of millions of Americans. As shown in the chart below, in 2005, only 7% of all U.S. adults used at least one social media site, but that percentage rose to 68% by 2018. And while millions of consumers make use of other social media platforms like Twitter and Snapchat, Facebook "remains the primary platform for most Americans."[14]

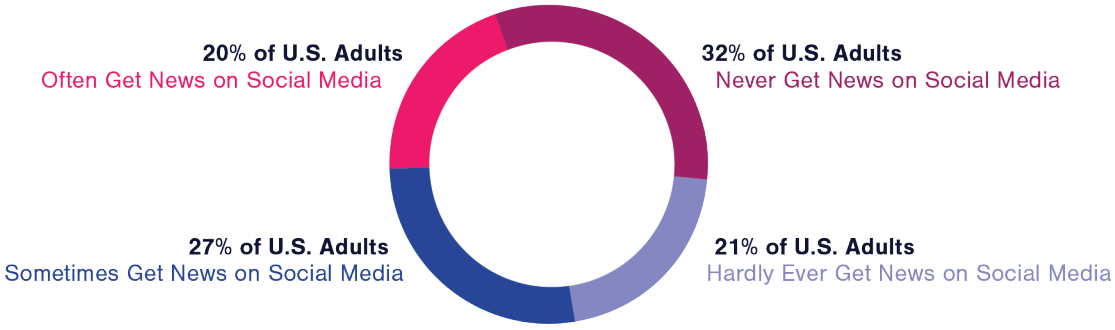
% of U.S. Adults Who Use Social Media



SOURCE: Pew Research Center, *Social Media Usage 2005-2015* (Oct. 2015); PEW Research Center, *Social Media Use in 2018* (Mar. 1, 2018).

Not only does social media play an important role in the social lives of Americans – U.S. teens report, for example, that social media helps strengthen friendships – but social media also helps inform consumers about news and potential purchases. More Americans get their news from social media platforms than from traditional newspapers.[15] Studies estimate that about 43% of U.S. adults get news from Facebook, which has the greatest usage among U.S. consumers.[16] But a large number of U.S. adults also get news from other social media platforms such as YouTube (21%), Twitter (12%), Instagram (8%), and Reddit (5%).

% of U.S. Adults Who Get News on Social Media ....



SOURCE: Pew Research Center, NEWS USE ACROSS SOCIAL MEDIA PLATFORMS 2018 (Sep. 10, 2018).

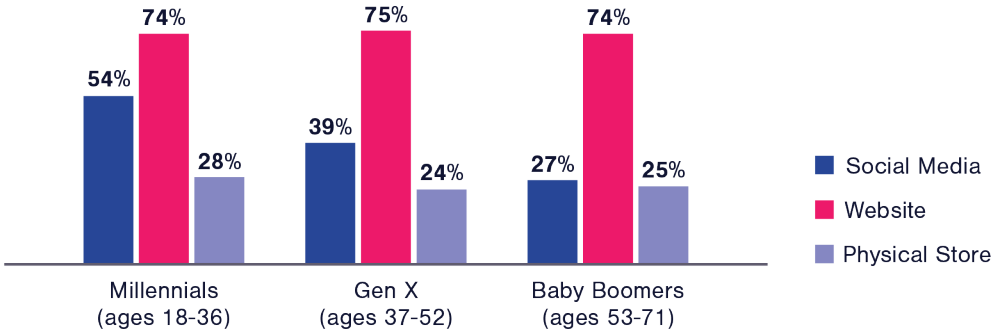
14. Pew Research Center, *Social Media Use in 2018* (Mar. 1, 2018).

15. Pew Research Center, *Social media outpaces print newspapers in the U.S. as a news source* (Dec. 2018). Pew reports that 20% of U.S. adults get their news from social media sites, while only 16% get their news from traditional print newspapers.

16. Pew Research Center, *10 Facts about Americans and Facebook* (Feb. 1, 2019). Pew reports that "no other major social media platform comes close to Facebook in terms of usage.

Social media platforms have also evolved into important tools for U.S. consumers wishing to buy products and services. As shown in the chart below, ***more U.S. adult consumers use social media platforms to research retail purchases than traditional in-store visits.*** The trend toward social media for researching retail purchases is strongest among Millennials – 54% of U.S. adult consumers ages 18 to 36, as defined in a Salesforce report in 2017, research potential purchases using social media. Businesses are increasingly recognizing the importance of social media platforms in connecting with customers and making sales. Retail experts estimate that "[n]early 25% of business owners are selling through Facebook and 40% are using social media as a whole to generate sales."[17] And independent studies show that Facebook is the leading application used by U.S. consumers during their online shopping sessions.[18]

Channels Consumers Use to Research Retail Purchases



SOURCE: SalesForce Research, 2017 CONNECTED SHOPPERS REPORT, *Shoppers Say So Long to the Linear Path to Purchase,* pg. 2 (Oct. 2018). The above chart contains excerpted data to show U.S. consumer use of social media, websites, and traditional in-store visits. The SalesForce survey of U.S. adults also presents data for consumers who use email, retailer mobile apps, text, and other methods for researching retail purchases.

Search engines have had a huge impact on the online activities of U.S. consumers. An estimated 233.9 million people in the U.S. used search engines in 2018, an increase of nearly 10% over the 213.6 million U.S. search engine users in 2014.[19] In the United States, Google has long been the dominant search engine in the marketplace. For the past few years, consumers in the U.S. have used Google to make approximately 10 billion search queries each month.[20] Recent studies estimate that, in the United States as of January 2019, Google has approximately 82% of the market share of desktop search traffic and nearly 95% market share for mobile search queries.[21]

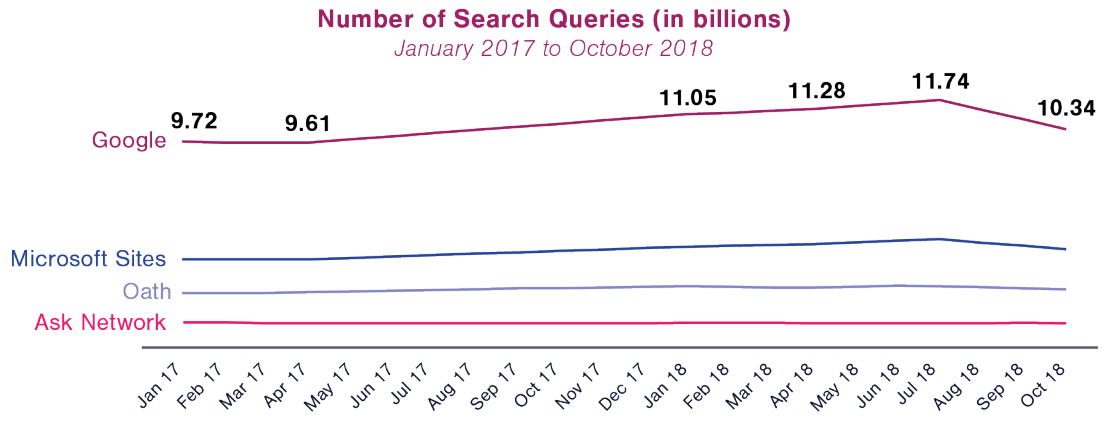
17. Fortune, Andrew Arnold, *Are We Entering the Era of Social Shopping?* (Apr. 4, 2018).

18. Statista, ONLINE SHOPPING BEHAVIOR IN THE UNITED STATES, *Occurrence of leading apps during a shopping session for online shoppers in the United States as of December 2017,* pg. 50 (2019). Verto Analytics estimates that Facebook is the leading app used during online shopping sessions, accounting for approximately 8% of all such occurrences.

19. U.S. DIGITAL USERS EMARKETER FORECAST 2016, pg. 19 (2016).

20. Comscore Search Engine Market Share rankings January 2017 through October 2018 (desktop only).

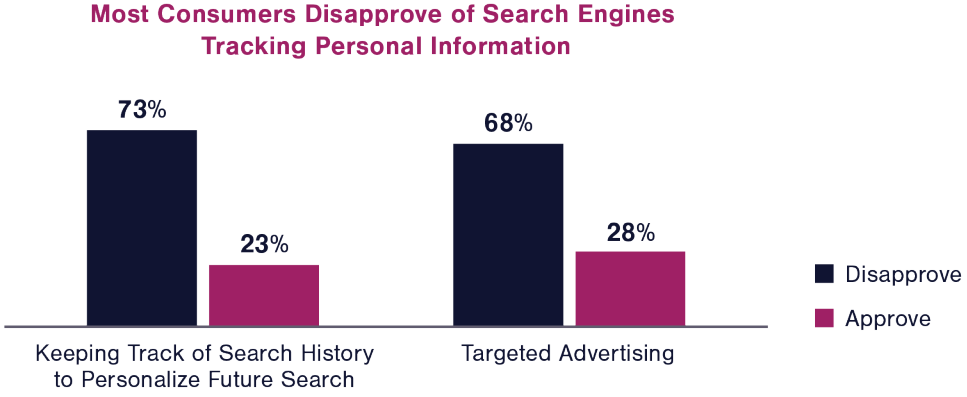
21. StatCounter GlobalStats, *Search Engine Market Share United States of America,* January 2018 – January 2019 (available at http://gs.statcounter.com/search-engine-market-share).



SOURCE: Comscore Search Engine Market Share rankings January 2017 through October 2018 (desktop only).

Moreover, search engines play a significant role in online shopping for U.S. consumers. In 2018, 27% of online shoppers used search engines to locate local businesses every single day. Given its level of engagement, search engines are considered a highly effective way to reach consumers and to influence their purchasing decisions.

For years, U.S. consumers have expressed privacy concerns about tracking of their online search activities.[22] In a 2012 study of search engine use among U.S. adults, the Pew Research Center found that many search users expressed concerns about personal information being collected for search results or for targeted advertising. As shown in the chart below, ***most U.S. adults indicated in the Pew surveys that they did not approve of personalized search results or targeted advertising.***

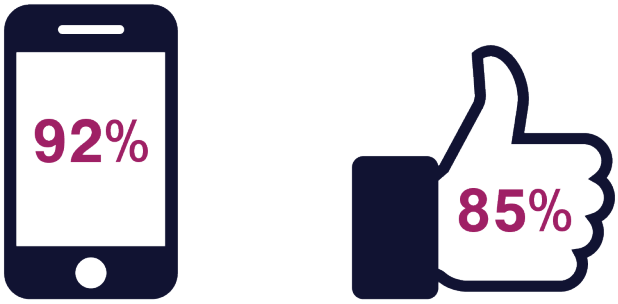


SOURCE: Pew Research Center, SEARCH ENGINE USE 2012.

22. *See, e.g.,* Pew Research Center, SEARCH ENGINE USE 2012 (Mar. 9, 2012) (noting that "strong majorities have negative views of personalized search results and targeted ads").

Not surprisingly, ***Millennials lead the trend of U.S. consumers that rely on and use social media in their daily lives.*** Study after study shows that Millennials – that is, Americans born between the years 1981 and 1996 and who (as of 2019) are between the ages of 23 and 38[23] – are more connected to the internet, more mobile (77.3% of U.S. adults aged 25-34 live in wireless-only households),[24] more engaged in online activities, and generally more comfortable with the flurry of technological advancements. As the chart below demonstrates, the Pew Research Center estimates that 92% of Millennials own a smartphone, and 85% of Millennial Americans use social media.

Millennial Americans Embrace Technology



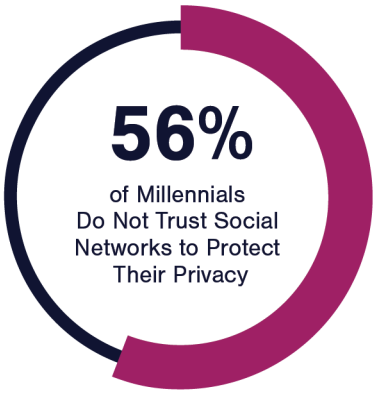
of Millennials Use Smartphones

of Millennials Use Social Media

SOURCE: Pew Research Center, *Millennials Stand Out for their Technology Use, but Older Generations Also Embrace Digital Life* (May 2, 2018).

But while Millennials appear comfortable with online activities like shopping and social media usage, they also have expressed reservations about how search and social media providers like Google and Facebook protect their data and personal information.

Most Millennials Do Not Trust Social Networks to Protect their Data and Information



SOURCE: eMarketer; Various Sources (Rad Campaign; Lincoln Park Strategies) (May 2018) (based on surveys of 1,000 adults in the U.S.).

23. Pew Research Center, *Defining Generations: Where Millennials End and Generation Z Begins* (Jan. 19, 2019).

24. Centers for Disease Control, National Center for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January – June 2018* (Dec. 27, 2018).

B. Regulatory Environment

A single, comprehensive federal law addressing consumer online privacy does not exist in the United States. Instead, today a patchwork of federal and state laws cover consumer online privacy – and for the most part, these laws were developed in the dial-up era before the widespread deployment of broadband connectivity, the broad appeal of social media platforms such as Facebook, and advances in computing technology and Artificial Intelligence (AI) that offer the capability to rapidly analyze vast amounts of data.[25] In the late 1990s, Congress passed a series of laws aimed at specific online issues and potential harms, as well as amended existing laws in light of new technology. As a result, a sector-by-sector patchwork approach developed to address consumer online privacy issues.[26]

The Federal Trade Commission has administered a technology-neutral framework for online privacy across all sectors for more than 20 years. The FTC's primary legal authority derives from the prohibition against unfair and deceptive practices in the marketplace found in Section 5 of the Federal Trade Commission Act, but the FTC also has specific legal authority to enforce a variety of sector-specific laws. As such, the FTC enforces specific statutes that protect consumer privacy and online data, such as personal health information, credit information, financial data, and children's information.[27] The FTC also enforces other relevant consumer protection laws that help safeguard consumers and their privacy.[28]

The FTC actively works to protect consumer online privacy through enforcement actions, consumer and business education programs, and policy initiatives specifically geared towards promoting privacy and security. As the cop on the privacy beat, the FTC has brought hundreds of privacy-related enforcement actions against a wide array of companies. The FTC has even focused its enforcement efforts on leading technology companies and edge providers such as Facebook, Google, and Twitter.[29] Actions involving other technology companies have afforded the FTC the opportunity both to apply a uniform approach to consumer online privacy and to develop deep expertise in protecting consumer interests in the internet ecosystem. In this regard, the FTC has addressed through enforcement actions a number of illegal privacy practices, including:

- Collecting information from children online without parental consent;
- Deceiving consumers about collection, use, and/or disclosure of their financial, health, video, and other personal information;
- Deceptively tracking consumers online;
- Publicly posting private data online without consumers' knowledge or consent.[30]

25. *See, e.g.,* Time, Keith Wagstaff, *How Target Knew A High School Girl Was Pregnant Before Her Parents Did* (Feb 17, 2012) (describing how the department store chain collected and analyzed consumer information). The magazine article describes how, with shopping data culled through its computers, the department store chain assigned a "pregnancy prediction" score to individual consumers and then sent targeted coupons in the mail based on these scores.

26. *See, e.g.,* 15 U.S.C. §1681-81t. The Fair Credit Reporting Act of 1970, as amended by the Fair and Accurate Credit Transactions Act of 2003, sets forth rights for individuals and responsibilities for consumer credit reporting agencies; 42 U.S.C. § 1320d note, The Health Insurance Portability and Accountability Act of 1996 adopted the HIPAA Privacy Rule as the national standard for the protection of individually identifiable health information. Enhanced HIPAA penalties were adopted in the Health Information Technology for Economic and Clinical Health Act of 2009. Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C § 6501 et seq. (addressing the collection of personal information from children under the age of 13). Sector-specific laws apply to various other business sectors.

27. *See, e.g.,* Health Breach Notification Rule, 16 C.F.R. Part 318; Fair Credit Report Act, 15 U.S.C. § 1681; Privacy of Consumer Financial Information, 16 C.F.R. Part 313; Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 et seq., and the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312.

28. *See, e.g.,* Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) Act, 15 U.S.C. § 7701 et seq., and the implementing rule, 16 C.F.R. Part 316.

29. *See, e.g.,* Federal Trade Commission, *Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Appel's Safari Internet Browser,* Press Release (Aug. 9, 2012); Federal Trade Commission, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises,* Press Release (Nov. 29, 2011); Federal Trade Commission, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information, Press Release (Mar. 11, 2011).

30. *See, e.g., United States v. VTech Elec. Ltd.,* No. 1:18-cv-114 (N.D. Ill. Jan. 8, 2018); *PayPal, Inc.,* No. C-4651 (F.T.C. May 23, 2018); Compete, Inc., No. C-4384 (F.T.C. Feb. 20, 2013); Jerk, LLC, No. 9361 (F.T.C. Apr. 2, 2014).

The FTC has filed over 100 enforcement actions regarding online privacy matters in the past 10 years.[31] Some of the FTC's more high-profile online privacy cases involved how leading edge providers misused the personal information of consumers. In 2011, Facebook settled with the FTC over consumer privacy charges. Specifically, the FTC charged that Facebook deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public. The FTC required Facebook to take several steps to ensure future compliance, such as providing prominent notice and obtaining express consent from consumers before sharing their information beyond their established privacy settings.[32] Also in 2011, the FCC finalized a settlement with Twitter, Inc. concerning charges that Twitter deceived consumers and put their privacy at risk by failing to safeguard their personal information.[33] In 2012, the FTC approved a consent order imposing a $22.5 million civil penalty on Google, Inc. for violating the privacy expectations of consumers.

Specifically, the FTC found that Google had tracked users of iPhones, iPads, and Mac computers by circumventing privacy protections on the Safari web browser.[34]

Besides enforcement action, the FTC works to educate consumers and businesses about consumer online privacy tools and compliance requirements. Recently, the FTC has focused on educational efforts regarding information security, mobile apps and health data, geolocation and children's privacy issues, among other areas. And the FTC also undertakes various policy initiatives intended to promote privacy and security, such as workshops and issue-specific reports.[35]

Telecommunications has been one area with certain existing sector-specific privacy rules. When Congress enacted sweeping legislation to transform the telecommunications industry in 1996, it created a framework in section 222 to govern telecommunications carriers' protection and use of information obtained by virtue of providing a telecommunications service.[36] When section 222 was adopted, the internet was a nascent technology – the vast majority of consumers accessed the internet through dial-up connections with their desktop computers, mobile phone deployment was in its early stages, and social media platforms were nonexistent. By its plain language, section 222 imposed a general duty on "telecommunications carriers" to protect the confidentiality of "customer proprietary network information" (CPNI), as well as other provisions intended to guard against the risk of anticompetitive behavior as the monopoly-dominated voice telecommunications market transformed into a competitive market, while also protecting the privacy expectations of consumers with respect to their call records.[37]

31. Government Accountability Office, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY, Appendix II (Jan. 2019) (detailing FTC enforcement cases covering online privacy matters since 2008). Since the GAO released its report in January 2019, the FTC has announced additional privacy-related enforcement action. See Federal Trade Commission, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law,* Press Release (Feb. 27, 2019).

32. Federal Trade Commission, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises* (Nov. 29, 2011).

33. Federal Trade Commission, *FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information* (Mar. 11, 2011).

34. Federal Trade Commission, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (Aug. 9, 2012); The Guardian, Charles Arthur, *Google to pay record $22.5 million fine to FTC over Safari tracking* (Aug. 9, 2012). Also in 2012, the FCC found in 2012 that Google had collected consumer personal information without permission, and issued a forfeiture based on Google's failure to cooperate in its investigation. The Guardian, Charles Arthur, *Google fined by FCC over Street View* (Apr. 16, 2012).

35. The FTC routinely publishes information about its privacy and data security efforts. *See, e.g.,* Federal Trade Commission, PRIVACY & DATA SECURITY UPDATE: 2018 (Mar. 2018) (available online at https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf); Federal Trade Commission, PRIVACY & DATA SECURITY UPDATE: 2017 (Jan. 2018); Federal Trade Commission, PRIVACY & DATA SECURITY UPDATE: 2016 (Jan. 2017).

36. 47 U.S.C. § 222.

37. In implementing section 222 over the course of years, the FCC adopted a number of orders addressing various aspects of CPNI and the obligations of telecommunications carriers. *See generally* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, CC Docket No. 96-115; WC Docket No. 04-36, *Report and Order and Further Notice of Proposed Rulemaking,* 22 FCC Rcd 6927, 6953, paras. 4-9 (2007) *(EPIC CPNI Order), aff'd sub nom. Nat'l Cable & Telecom Assoc. v. FCC,* No. 07-132 (D.C.Cir. decided Feb. 13, 2009).

In 2016, the FCC took the step of expanding the CPNI regime to apply to broadband internet service providers (ISPs). In this regard, the FCC adopted privacy rules that collided with the FTC's long-established privacy regime. In particular, the FCC established a broad "opt-in" regime that applied to ISPs that required, among other things, that ISPs obtain affirmative "opt-in" consent from consumers to use and share their information.[38] The FCC's new privacy framework did not apply to edge providers that collect large amounts of information on consumer online activity.[39]

Recognizing the imbalance that the FCC's new rules created, Congress overrode the FCC CPNI regulations in a Joint Resolution adopted in April 2017.[40] As a result of Congress's action, the FCC's privacy regime was never implemented, and privacy enforcement was restored to the FTC. Through formal procedures, the FTC and the FCC coordinate their privacy enforcement efforts, where appropriate.[41]

Because of widespread consumer privacy concerns, state legislatures are taking steps to adopt state-specific laws addressing consumer online privacy. Most notably, last year California adopted an expansive privacy law, the California Consumer Privacy Act (CCPA) of 2018. In brief, the CCPA took sweeping steps to provide California residents a wide array of new rights, such as the right to know what personal information a business has collected, the right to opt out of allowing a business to sell their personal information, the right to request deletion of personal information, the right to receive equal service and pricing, and the right to access personal information in a "readily usable format" that enables its transfer to third parties without hindrance.[42] The California law – which is not limited to information collected over the internet – also addressed other issues, such as creating broad definitions of consumer, business, and personal information, and authorizing the California Attorney General to promulgate regulations to further the statute's purpose.

Although significant attention has been placed on the California Consumer Privacy Act of 2018, many other states have taken or are in the process of considering new measures related to consumer privacy and security of online information.[43] For example, Vermont enacted a consumer online privacy law aimed towards data brokers that include registration requirements, disclosure requirements, and opt-out provisions, among other things.[44] Many other states have taken steps to enact privacy laws or are considering doing so. The National Conference of State Legislatures (NCLS) reports that "close to half the states" are considering taking action "to restrict how internet service providers can collect or share consumer data."[45] And state attorney generals are also moving to enforce data privacy law against edge providers and others.[46]

38. In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16- 106, *Report and Order,* 31 FCC Rcd 13911 (2016).

39. *See id.* at paras. 28-40.

40. Joint Resolution, Pub. L. No. 155-22 (2017) ("Resolved by the Senate and House of Representatives of the United States of America in Congress assembled, That Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274 (December 2, 2016)), and such rule shall have no force or effect.").

41. *See* Federal Communications Commission, *Restoring Internet Freedom FTC-FCC Memorandum of Understanding,* DOC-348275 (Dec. 14, 2017).

42. *See* California Assembly Bill No. 375, California Consumer Privacy Act of 2018. Details of the California law, including links to the text of the law and other information, is available on the California Attorney General's website (https://www.oag.ca.gov/privacy/ccpa); The National Law Review, *Updates to Massachusetts Breach Notification Law – Much More Than Mandatory Credit Monitoring* (Jan. 13, 2019).

43. *See, e.g.,* MediaPost Communications, Wendy Davis, *Washington State Lawmakers Consider Privacy Bill* (Jan 22, 2019); Consumer Reports, James K. Wilcox, *States Push Their Own Internet Privacy Rules* (Apr. 20, 2017); GovTech Magazine, *10 States Take Internet Privacy Matters Into Their Own Hands* (Apr. 10, 2017).

44. Vermont's Act 171 of 2018, 9 V.S.A. §§ 2430, 2433, 2446, and 2447; *see* Vermont Office of the Attorney General, *Report to Vermont General Assembly on Data Privacy* (Dec. 15, 2018) (noting efforts by other states to adopt privacy laws and recommending additional statutory measures in Vermont); VT Digger, Xander Landen, *AG says Vermont should take more steps to protect data privacy* (Dec. 30, 2018); Bloomberg Law, Sara Merken, *Vermont Law Rings in Registration, Disclosure for Data Brokers* (Dec. 27, 2018) (describing Vermont law as "the first of its kind in the country").

45. National Conference of State Legislatures, *Privacy Legislation Related to Internet Service Providers* (Nov. 16, 2018) (available at http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx); *see also* National Conference of State Legislatures, State Laws Related to Internet Privacy (Feb. 8, 2019) (available at: http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx).

46. *See* The Washington Post, Tony Romm, Brian Fung, Aaron C. Davis, and Craig Timberg, *It's About Time: Facebook Faces First Lawsuit from U.S. Regulators After Cambridge Analytica Scandal* (Dec. 19, 2018) (describing lawsuit filed by DC Attorney General against Facebook for consumer privacy violations); GovTech, *New Mexico AG Files Lawsuit Alleging Tech Companies Illegally Track Children* (Sep. 13, 2018); *see also Rosenbach v. Six Flags Entertainment Corp.,* Docket No. 123186 (Illinois Jan. 25, 2019) *(Rosenbach v. Six Flags).* In Rosenbach v. Six Flags, the Illinois Supreme Court ruled that, when companies collect consumer biometric data (e.g., fingerprints) without informed opt-in consent, they can be sued even without proof of injury or harm due to the data collection.

Consumer privacy concerns do not stop at the nation's border, of course. In May 2018, European regulators started full implementation of the General Data Protection Regulation (GDPR) as a uniform framework for addressing consumer online privacy matters in the European Union.[47] Privacy regulators in Europe specifically pointed to the data misuse issues raised in the Facebook/Cambridge Analytica matter to support the rollout of the GDPR.[48] In addition, European privacy regulators have taken steps to enforce their privacy laws through fines and forfeitures. Just this year, French regulators fined Google $57 million for violating the GDPR.[49] The fine against Google follows similar enforcement action aimed at Facebook in late 2018 by the privacy watchdog in the United Kingdom.[50]

In light of the issues and attention focused towards consumer online privacy, industry groups and other stakeholders in the U.S. are actively developing consensus-based approaches and a uniform framework for federal legislation and policy initiatives. Numerous industry coalitions and groups have released draft principles and recommendations for federal legislation that would balance protecting consumer privacy interests with incentivizing innovation.[51] And recently, the Government Accountability Office (GAO) completed another review of U.S. internet privacy efforts at the federal level.[52] This GAO effort followed previous examinations into internet issues that included consumer privacy, including in the context of the Internet of Things (IoT) and connected vehicles.[53] In its report, the GAO recommends that Congress "consider developing comprehensive legislation on internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving internet environment."[54]

47. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL f 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation); *see* European Commission, *Statement by Vice-President Ansip and Commissioner Jourova Ahead of the Entry Into Application of the General Data Protection Regulation* (May 24, 2018) (http://europa.eu/rapid/press-release_STATEMENT-18-3889_en.htm); European Commission, *Joint Statement by First Vice-President Timmermans, Vice-President Ansip, Commissioners Jourova and Gabriel Ahead of Data Protection Data* (Jan. 25, 2019) (providing a summary of GDPR and activities since adoption) (http://europa.eu/rapid/press-release_STATEMENT-19-662_en.htm).

48. *See* European Commission, *A New Era for Data Protection in the EU* (May 2018) (noting that the "Facebook/Cambridge Analytica revelations" support the adoption of the GDPR) (https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes_en.pdf).

49. Wall Street Journal, Sam Schechner, *Google Fined $57 Million in Biggest Penalty Yet Under New European Law* (Jan. 21, 2019); The New York Times, Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law* (Jan. 21, 2019).

50. The Guardian, Jim Waterson, *UK Fines Facebook £500,000 for Failing to Protect User Data* (Oct. 25, 2018) (reporting UK fine against Facebook in connection with the Cambridge Analytica scandal). Facebook remains under investigation and news outlets report that it could be facing a substantially larger fine. *See* Wall Street Journal, Sam Schechner, *Facebook Faces Potential $1.63 Bill Fine in Europe Over Data Breach* (Sep. 30, 2018).

51. *See, e.g.,* Business Software Alliance, *BSA Privacy Framework* (available at the following website: https://www.bsa.org/~/media/Files/Policy/BSA_2018_PrivacyFramework.pdf); Information Technology Industry Council, *Framework to Advance Interoperable Rules (FAIR) on Privacy* (available at the following website: https://www.itic.org/dotAsset/feb6ab98-7c3b-421b-9f92-27528fa4c4f2.pdf); The Internet Association, Policy Position: Privacy (https://internetassociation.org/positions/privacy/); U.S. Chamber of Commerce, *U.S. Chamber Privacy Principles* (Sep. 2018) (https://www.uschamber.com/issue-brief/us-chamber-privacy-principles); Google, Inc., *Framework for Responsible Data Protection Regulation* (Sep. 2018) (available at the following website: https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf).

52. Government Accountability Office, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY (Jan. 2019) (GAO INTERNET PRIVACY REPORT).

53. Government Accountability Office, VEHICLE DATA PRIVACY (Jul. 2017); Government Accountability Office, INTERNET OF THINGS (Jul. 2017).

54. GAO INTERNET PRIVACY REPORT at 37. The GAO conducted previous reviews of internet privacy issues at the federal level in 2017.

III. Consumer Personal Information in the Internet Ecosystem

Companies that operate at the "edge" of the internet and provide services directly to broadband users collect large amounts of consumer data. Search engines, social media sites, and e-commerce platforms are among the most heavily-used edge provider platforms in the internet ecosystem.

Edge providers collect and use personal information from consumers to provide their online services and to facilitate internet-enabled products. In fact, ***studies show that edge providers collect and use more personal information than the ISPs that provide broadband and other connections to the internet.***[55] In serving U.S. consumers, edge providers collect and track across multiple platforms information on consumers, such as search terms, social and professional networks, political attitudes, preferences and tastes, likes and dislikes, beliefs, location and usage patterns, as well as information traditionally considered to be sensitive, such as contact and financial information. ***With their broad access to the activity of consumers using their websites and applications, edge providers gather information that many then monetize through targeted advertising.***

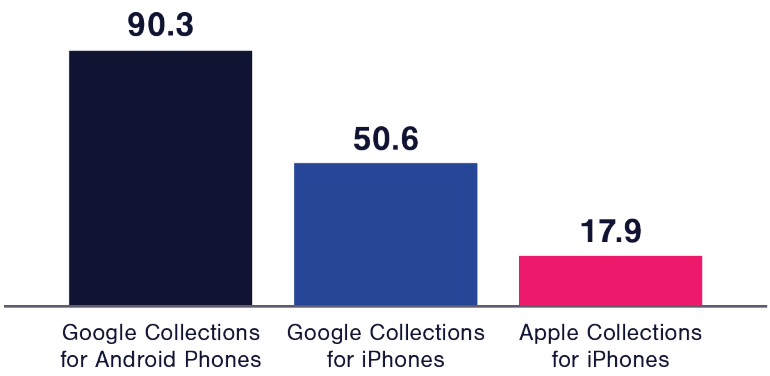
The vast frequency and scope of edge providers' consumer data collection is illustrated in a 2018 analysis of Google's data collection practices.[56] As shown in the following chart, ***independent researchers found that Google collected extensive information about consumer online activities, and did so on a near-continuous basis using both active and passive means*** – from Android phones an average of 90 times per hour; and for Apple iPhones, Google collected consumer information about their phone usage on average about 50 times per hour. Over the course of one day, the study showed that Google collected between 5.7 MB to 11.6 MB of data, including location information, app store usage, ad domains, and device uploads, among other types of information.[57]

55. *See, e.g.,* The Institute for Information Security & Privacy at Georgia Tech, Peter Swire, ONLINE PRIVACY AND ISPS: ISP ACCESS TO CONSUMER DATA IS LIMITED AND OFTEN LESS THAN ACCESS BY OTHERS (2016) (ONLINE PRIVACY STUDY).

56. Prof. Douglas C. Schmidt, Vanderbilt University, *Google Data Collection* (Aug. 15, 2018) *(Google Data Collection Study).*

57. *Google Data Collection Study* at Figure 12. The Google Data Collection Study assessed Google's collection of consumer data during a consumer's "typical day of use" and during a day when the mobile phones were idle. Id. at Figure 6. During days of "idle use," Google's consumer data collection amounted to roughly half the data collected during a "typical day of use" (*e.g.,* 40.2 requests per hour for a total of 4.4 MB of data per day when Android phones were idle).

Frequency of Google's Data Collection per Device per Hour



SOURCE: *Google Data Collection Study* at Figure 12 (information requests from mobile devices during a typical day of use).

Not only are the frequency and volume of edge provider data collection significant, but their ***data collection is extraordinarily intimate in terms of the insights and observations about consumers.*** Another 2018 study of data collection among edge providers highlighted the broad categories of data collected by Google, including search history, browsing history, media preferences, location, movement and travel, social activity, communications, documents, device usage, and (with the foray into "smart" home monitoring and control device) residential activity.[58] Similarly, the nature of Facebook's service offerings provide the edge provider a "powerful trove of consumer data," such as social relationships, activity, location, personal photos, interests, likes/dislikes, beliefs, private communications, and calendar/schedule information.[59] And consumer tracking and data collection is not limited to occasions when consumers use an edge provider's service directly. With the use of cookies, application programming interfaces (APIs), and other methods, edge providers such as Facebook and Google are able to track consumer activity across the internet and can even "consistently identify" consumers using other websites and applications.[60]

And the level of intimacy in the data that is collectable has reached "unprecedented" levels with the help of machine learning and artificial intelligence. Studies have shown that, when using Google and other search engines, U.S. consumers search the internet "as if unobserved."[61] Under this assumed veil of anonymity, consumers conduct a wide variety of searches that reveal traits such as sexual orientation, medical conditions, hidden social biases, and potentially even criminal behavior. Personal consumer data that edge providers collect can be used to make surprisingly accurate predictions of the private details of people's lives. For example, one study employed machine learning techniques to show that anonymous social relationship data gleaned from Facebook users can (more often than not) accurately predict the identity of romantic partners.[62] Similarly, queries with Google and other search engines can be used to identify not just social trends, but key intimate details about a person's life that can raise issues of potential exploitation from such data.[63]

58. Michael Kearns, *Data Intimacy, Machine Learning, and Consumer Privacy,* 5-7 (Penn. Law/CTIC 2018) (available at https://www.law.upenn.edu/live/files/7952-kearns-final.pdf) (Data Intimacy Study).

59. *See Data Intimacy Study* at 7-8.

60. *See Data Intimacy Study* at 9 (describing "fingerprinting" properties of allegedly anonymous search queries); N. Cameron Russel, Florian Schaub, Allison McDonald, William Sierra-Rocafort, Fordham Center on Law and Information Privacy, APIs and Your Privacy (Jan. 2019) (https://ir.lawnet.fordham.edu/faculty_scholarship/916/).

61. *Data Intimacy Study* at 9 (citing Seth Stevens-Davidowitz, Doctoral Thesis, Harvard University), Essays Using Google Data 2013 (available at the following website: https://dash.harvard.edu/bitstream/handle/1/10984881/StephensDavidowitz_gsas.harvard_0084L_11016.pdf?se quence=1).%25C2%25A0).

62. *Data Intimacy Study* at 13.

63. *Data Intimacy Study* at 9-10; see The Washington Post, Caitlin Dewey, *You Are What You Google Search* (Dec. 16, 2014); The Washington Post, Caitlin Dewey, *Everything Google Knows About You (And How It Knows It)* (Nov. 19, 2014). In her article, Ms. Dewey notes that

> According to Google, I am a woman between the ages of 25 and 34 who speaks English as her primary language and has accumulated an unwieldy 74,486 e-mails in her life. I like cooking, dictionaries and Washington, D.C. I own a Mac computer that I last accessed at 10:04 p.m. last night, at which time I had 46 open Chrome tabs.

Id. For information about social trends revealed through Google searches, see Pew Research Center, *What Google Searches Can Tell Us About Americans' Interest in Guns* (Mar. 16, 2018); Pew Research Center, *Searching for News: The Flint Water Crisis* (Apr. 27, 2017) (http://www.journalism.org/essay/searching-for-news/); The Washington Post, Christopher Ingraham, *What Our Google Searches Reveal about the Drug Epidemic* (Jul. 31, 2017).

By contrast, a detailed working paper issued by The Institute for Information Security & Privacy (IISP) at Georgia Tech concluded that ISPs do not have comprehensive access to data about individual consumers because of technological limitations.[64] The study also reported that other companies often have access to more information and a wider range of information than ISPs, which means that ISPs do not have unique access to consumer information.

Several technological developments place substantial limitations on the ability of ISPs to monitor and track the online activities of U.S. consumers. First, multiple mobile devices and connections greatly limit ISP visibility into consumer online activity, because consumers may be connecting to the internet using multiple different networks and ISPs, such as the home broadband provider, their mobile broadband connection, any number of WiFi providers at various hotspots, and the broadband provider at work. Mobile devices, in particular, often switch between ISPs throughout the day.[69] Furthermore, in light of the competitive broadband marketplace, consumers frequently switch broadband providers – the FCC estimates that roughly one-sixth of U.S. consumers switch ISPs every year, and more than a third switch every three years.[70] The U.S. consumer's tendency to periodically change ISPs splinters information on their total internet activity, diminishing the picture that ISPs can track. Edge providers, however, continue to maintain a more accurate, comprehensive, and up-to-date view. The IISP study found that, as consumers become "more mobile and use multiple devices," ISPs receive less and less information about their online activity. At the time of the IISP online privacy study, the average internet user had 6.1 connected devices; more current studies show that, as of 2017, there are 8.1 connected devices per capita in the United States, and that figure is expected to grow to 13.6 connected devices by 2022.[65] Other technological developments that limit ISP visibility into consumer online activities are the pervasive use of encryption that blocks visibility into consumer online activity (e.g., the HTTPS version of the basic web protocol) and the shift in domain name lookup facilitated by the proliferation of Virtual Private Networks (VPNs) and other proxy services.[66]

Cross-context tracking and cross-device tracking are critical capabilities for any one company to have in order to gain meaningful insight into consumers' online activity and behavior.[67] In both cases, edge providers and others dominate ISPs. The ability to combine consumer online activity from multiple contexts – for example, from social networks, search queries, webmail, browser history, internet video, and e-commerce – provides unique and commercially valuable insights.

64. IISP ONLINE PRIVACY STUDY at 3-4, 23-41.

65. IISP ONLINE PRIVACY STUDY at 3; *see* Cisco, Visual Networking Index, *VNI Forecast Highlights Tool* (2018) (estimating % of internet users, devices per capita, average speed, and more in the United States 2017-2022) (available at https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html#). In its most recent Visual Networking Index, Cisco estimated 8.1 devices per capita in the United States as of 2017, and expected that there would be 13.6 internet-connected per capita in the U.S. by 2022.

66. IISP ONLINE PRIVACY STUDY at 3-4.

67. IISP ONLINE PRIVACY STUDY at 66-67, 100-21. Cross-context tracking is what occurs when an online company tracks two or more types of data, such as search engine queries and web browser history or social networks overlaid with an advertising network. *Id.* at 101-02. Cross-device tracking is the capability to map consumers as they move between devices, e.g., from desktop, to tablet, to game console, to work computer, to smartphone. *Id.* at 116-17.

68. *Id.* at 103-06.

69. *Id.* at 120-21.

IV. The Millennial Generation and CivicScience Consumer Online Privacy Survey

Millennial Americans are an important segment of the U.S. population, and many assumptions have been made regarding their views about their privacy online.[70] The U.S. Census Bureau estimates that Americans born between 1982 and 2000 number more than 83 million people and represent more than a quarter of the nation's population.[71] Millennials are also now "the largest generation in the U.S. labor force," comprising more than a third of all U.S. workers.[72] Numerous studies report that Millennials in the U.S. are more diverse, more educated, and more comfortable with technology than preceding generations.[73] Millennials in the U.S. also rely on mobile communications more so than other generations, and use their mobile devices for a wide range of online activities, including checking/posting on social media, streaming videos and/or music, buying or selling items, or reading/watching news and sports.[74]

To examine the privacy views of Millennials and other U.S. consumers, the Internet Innovation Alliance (IIA) commissioned an independent market research survey to determine the views and preferences of Millennial consumers in the U.S. about consumer online privacy. CivicScience – a leading and independent polling, market research and data analytics firm – designed and conducted a comprehensive, statistically-valid survey of consumers in the United States in April 2019. CivicScience performs its market research online, running highly accurate, micro-survey polling applications embedded within a website's native content experience. The company uses a quota-based sampling methodology, which ensures that respondent groups are precisely representative of the U.S. population by demography and geography. CivicScience delivered its survey to "a random quota-based sample of a minimum of 8,000 online U.S. adult respondents aged 18 or older."[75] The CivicScience report notes that respondents participated voluntarily and for no financial or other extrinsic reward, which "significantly reduces" potential bias in the polling results.

CivicScience crafted its survey to provide greater insight into the views of consumers about their online data privacy. The specific four questions that CivicScience asked at random were:

1. ***I'm worried about my personal financial information, including social security number and banking information, being hacked from the online tech and social media companies I use.***
2. ***I'm OK with online tech/social media companies that collect and use my personal data because it makes my online searches, advertisements and content more relevant to me.***
3. ***I'm concerned about how tech/social media companies are using my online data and location information for commercial purposes.***
4. ***There should be a single, national policy addressing consumer data privacy rules in the United States.***

70. Federal Communications Commission, *Broadband Decisions: What Drives Consumers to Switch – Or Stick With – their Broadband Internet Provider,* Working Paper, DOC-303264A1 (Dec. 2010).

71. Sarah Landrum, Forbes, *"Here's Why Millennials Are The Most Data-driven Generation,"* Article (Aug. 29, 2017).

72. U.S. Census Bureau, *Millennials Outnumber Baby Boomers and Are Fare More Diverse, Census Bureau Reports,* Press Release (Jun. 25, 2015).

73. Pew Research Center, *Millennials Are the Largest Generation in the U.S. Labor Force* (Apr. 11, 2018); Pew Research Center, *Millennials Approach Baby Boomers as America's Largest Generation in the Electorate* (Apr. 3, 2018).

74. *See, e.g.,* U.S. Chamber of Commerce, The Millennial Generation (2012); Pew Research Center, *Millennial Life: How Young Adulthood Today Compares with Prior Generations* (Feb. 14, 2019).

75. Centers for Disease Control, National Center for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January – June 2018* (Dec. 27, 2018) (reporting that over 77% of adults ages 25-34 live in wireless-only households); see CivicScience, Consumer Preferences for Internet Access and Online Activities Market Research Report, Question 2 and Question 3 Results (Jun. 27, 2018) (reporting the online activities for Millennial Americans and other U.S. consumers).

76. *See* CivicScience Consumer Data Privacy Concerns Report at 2 (May 2019).

Consumers were asked one or more of these four questions in random order and could respond that they Strongly Agree, Somewhat Agree, Neither Agree nor Disagree, Somewhat Disagree, or Strongly Disagree. Utilizing its extensive experience and background conducting market research, CivicScience provided detailed demographic information about consumer preferences based on the survey responses. In its report, CivicScience presented its findings as summary "topline results," but also detailed results based on age group (Millennial, Generation X, Baby Boom), gender, residential area (Urban, Suburban, Rural, and Other), race, and income. These market research results provide accurate information that can be used to assess consumer views about online data privacy at the nationwide level.

The results of the CivicScience Consumer Data Privacy Survey show that ***today's Millennial Americans are deeply concerned about the privacy of their online personal data.*** Even greater percentages of older Americans express concern about the privacy of their online data. Not surprisingly, the concerns of Millennials track those of millions of Americans who have experienced a rash of data breaches and witnessed first-hand the abuses and misuses of their personal data by actors in today's internet ecosystem. ***The survey results also show that today's Millennial Americans strongly support a single, national policy for protecting consumer online data privacy.*** Overall, a very strong majority – 72% of responding consumers – support a single, national online data privacy policy.

Two CivicScience survey questions home in on the privacy concerns of Millennials and other consumers. In Question 2, CivicScience asked consumers to respond to the statement "I'm OK with online tech/social media companies that collect and use my personal data because it makes my online searches, advertisements and content more relevant to me." In Question 3, consumers responded to the statement "I'm concerned about how tech/social media companies are using my online data and location information for commercial purposes." The results of the CivicScience Consumer Data Privacy Survey show that:

- ***More than two-thirds of Millennials (69%) are "not OK" that online tech and social media companies collect and use their personal data in order to make online searches, advertisements, and content more relevant to them.*** Nearly 8 in 10 older Americans – 77% of Generation Xers and 79% of Baby Boomers – are "not OK" with online tech/social media companies collecting and using their personal data to make online searches, advertisements, and content more relevant to them.

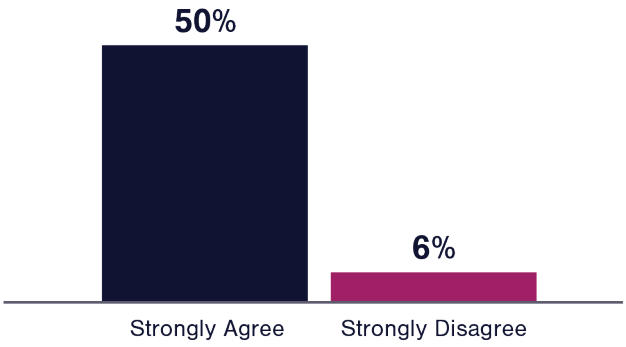
- ***Nearly three-quarters of Millennials (74%) are concerned about how online tech and social media companies are using their online data and location information for commercial purposes.*** Even more Generation Xers (75%) and Baby Boomers (79%) are concerned about how tech and social media companies use their online data and location information for commercial purposes.

The survey results also show that clear majorities of consumers of all ethnicities are generally "not OK" that online tech/social media companies collect and use their personal data to make their online searches, advertisements, and content more relevant to them. Over two-thirds of Hispanics (68%), nearly three-quarters of Blacks (73%), over three-quarters of Whites (77%), and fully 80% of Other consumers report that they Strongly Disagree or Somewhat Disagree with tech/social media companies collecting and using their personal data in this way. Not surprisingly, the survey results also indicate that consumers of all ethnicities are concerned about how tech/social media companies are using their online data and location information for commercial purposes. As shown in the chart below, most Hispanics (56%), Blacks (76%), Whites (81%), and those of Other ethnicities (81%) report that they are concerned with how tech/social media companies use their data.

The CivicScience Consumer Data Privacy Survey drills down on the level of concern Millennials have about how tech/social media companies are using their online data and location information for commercial purposes. As noted previously, CivicScience asked consumers to report to what degree they agree or disagree with the survey questions.

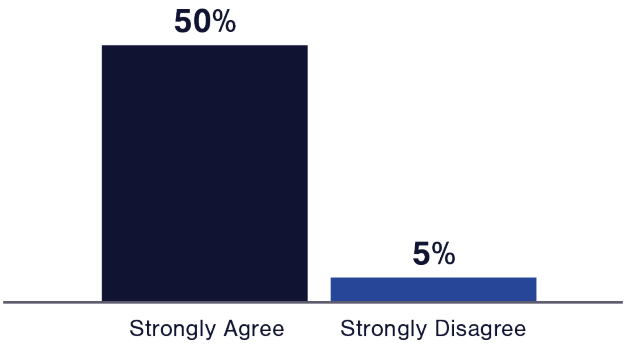
With respect to the CivicScience survey question about consumer concerns regarding the use of online data and location information for commercial purposes (i.e., Question 3), fully 50% of Millennials stated that they "strongly agree" with the statement of concern. A slightly larger percentage of older Americans shared the same level of intensity with their concerns as Millennials. By contrast, a mere 6% of Millennials "strongly disagreed" with the statement of concern. Similarly, fully 50% of Millennials strongly disagreed that they are "OK" with tech/social media companies collecting and using their personal data to make online searches, advertisements, and content more relevant to them, while only 5% of Millennials strongly agree that they are "OK" with these data collection practices. For both questions, about 10 times as many Millennial respondents reported a "strong" level of concern as those who reported that they "strongly" felt no concern. ***These imbalances indicate that very few Millennials fully trust the way in which tech/social media companies are using their online personal data and location information.*** The charts below illustrate these imbalances.

Concerned How Tech/Social Media Uses Personal Data & Location Information (For Millennials)



SOURCE: CivicScience Consumer Data Privacy Concerns, Question 3.

Not OK with Tech/Social Media Collecting & Using Personal Data (For Millennials)



SOURCE: CivicScience Consumer Data Privacy Concerns, Question 2.

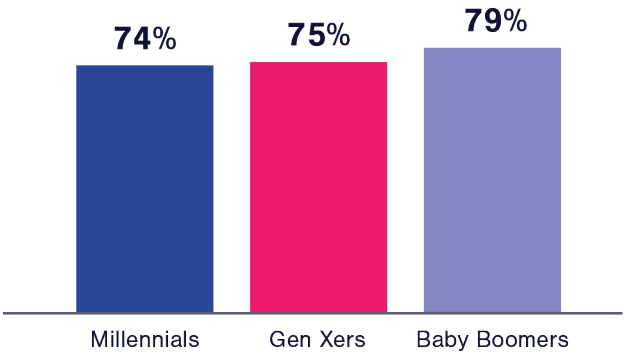
77. Note that the wording for CivicScience Question 2 states specifically, "I'm OK with online tech/social media companies that collect and use my personal data because it makes my online searches, advertisements, and content more relevant to me." In the survey, 50% of Millennial respondents reported that they Strongly Agree with the wording of the question while only 5% reported that they Strongly Disagree with the question. For the purposes of this chart, the white paper uses the terminology "Not OK" to remain stylistically consistent with other sections of this paper.

These privacy concerns are also shared among Americans of all income levels and living in all residential areas of the country. As shown in the charts below, a very strong majority of consumers of all income levels – 73% of those with annual incomes of less than $50,000, 79% of those with incomes between $50,000 and $100,000, and 81% of upper-income consumers are concerned about how tech/social media companies use their personal data and location information. Furthermore, roughly three-quarters and more of consumers at all income brackets are "not OK" with tech/social media collecting and using their personal data to make online searches, advertisements, and content more relevant to them. Not surprisingly, these concerns are evident among consumers living in all residential areas, although Suburban consumers are most likely (81%) to be "not OK" with the collection of their personal data.

CivicScience Question 3:

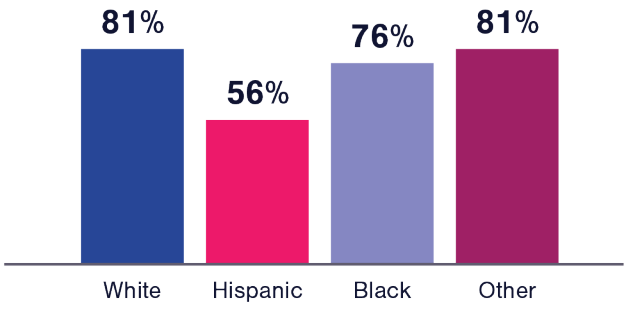
I'm concerned about how tech/social media companies are using my online data and location information for commercial purposes.

Concerned How Tech/Social Media Uses Personal Data & Location Information (By Generation)



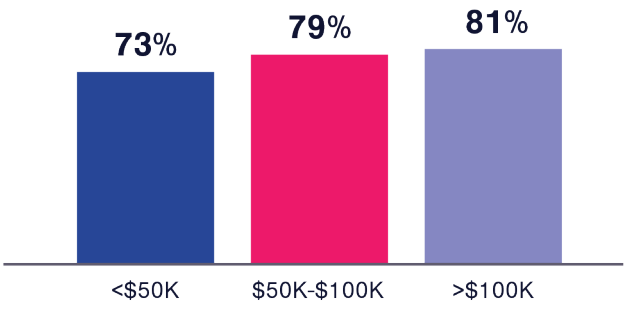
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 3.

Concerned How Tech/Social Media Uses Personal Data & Location Information (By Ethnicity)



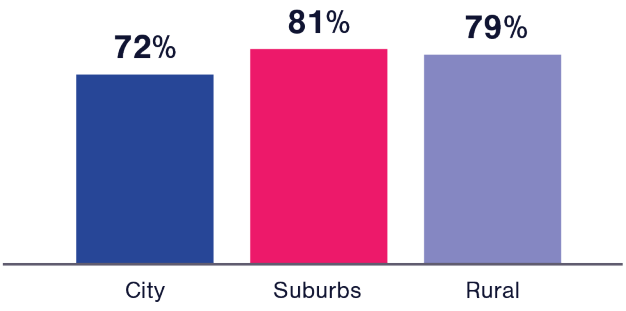
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 3.

Concerned How Tech/Social Media Uses Personal Data & Location Information (By Income)



SOURCE: CivicScience Consumer Data Privacy Concerns, Question 3.

Concerned How Tech/Social Media Uses Personal Data & Location Information (By Residential Area)

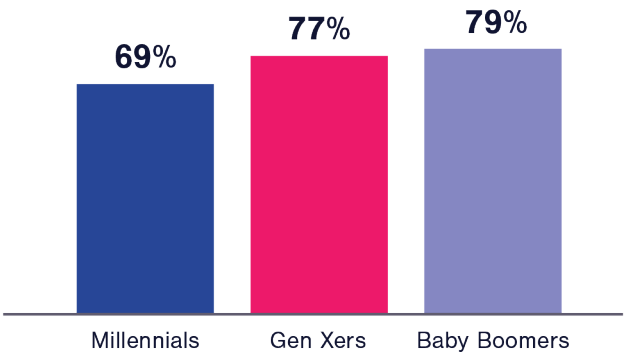


SOURCE: CivicScience Consumer Data Privacy Concerns, Question 3.

CivicScience Question 2:

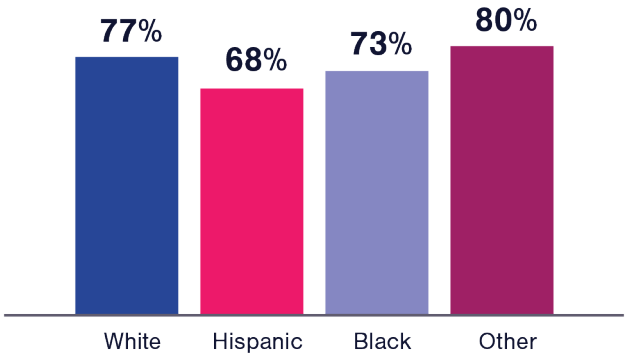
I'm OK with online tech/social media companies that collect and use my personal data because it makes my online searches, advertisements and content more relevant to me.

Not OK with Tech/Social Media Collecting & Using Personal Data (By Generation)



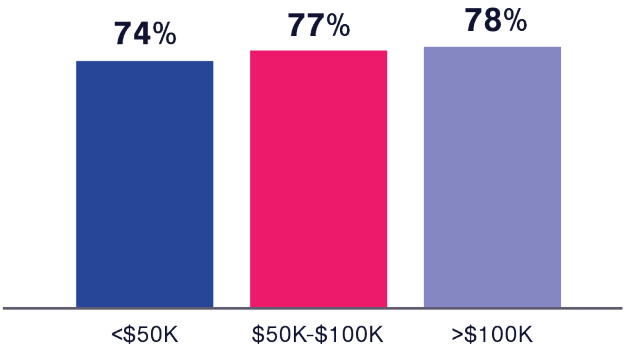
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 2

Not OK with Tech/Social Media Collecting & Using Personal Data (By Ethnicity)



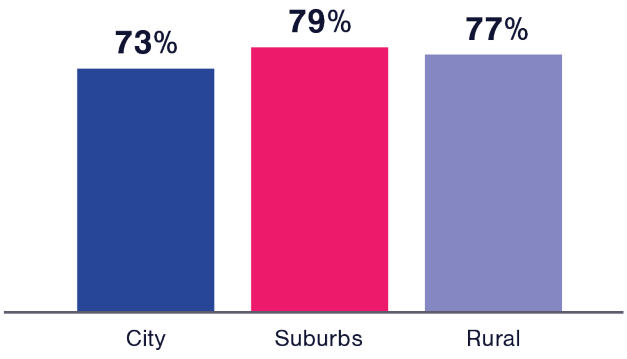
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 2

Not OK with Tech/Social Media Collecting & Using Personal Data (By Income)



SOURCE: CivicScience Consumer Data Privacy Concerns, Question 2.

Not OK with Tech/Social Media Collecting & Using Personal Data (By Residential Area)



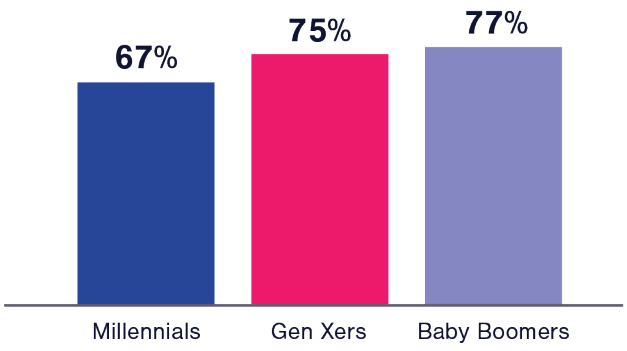
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 2

Consumer privacy concerns are based at least partly on worries about hacking of their personal financial information. More than two-thirds of Millennials (67%) worry about their personal financial information being hacked from online tech/social media companies. And even larger percentages of Generation Xers and Baby Boomers worry about their personal information being hacked. Indeed, ***concerns about hacking are shared by Hispanic, Black, and Other Americans.*** Over two-thirds of Hispanics (71%) and Blacks (71%) worry that their personal financial information may be hacked from online tech and social media companies. ***And these worries about hacking are shared by consumers living in all types of residential areas in the United States.*** Three-quarters of Americans living in the Suburbs (75%) and nearly as many Americans living in Rural Areas (71%) and Cities (72%) worry about their personal financial information being hacked from tech/social media companies.

CivicScience Question 1:

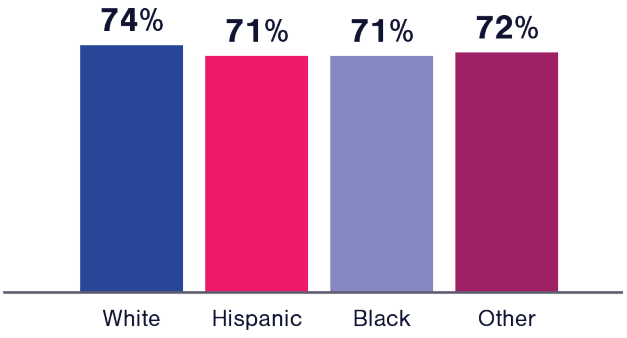
I'm worried about my personal financial information, including social security number and banking information, being hacked from the online tech and social media companies I use.

Worried about Hacking of Personal Financial Data (By Generation)



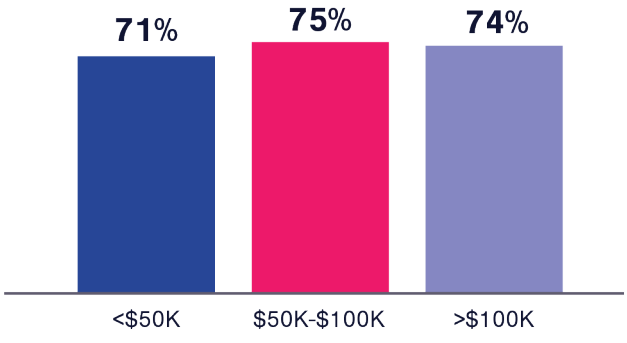
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 1.

Worried about Hacking of Personal Financial Data (By Ethnicity)



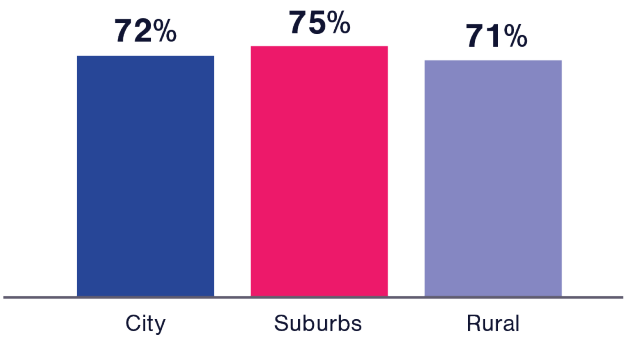
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 1.

Worried about Hacking of Personal Financial Data (By Income)



SOURCE: CivicScience Consumer Data Privacy Concerns, Question 1.

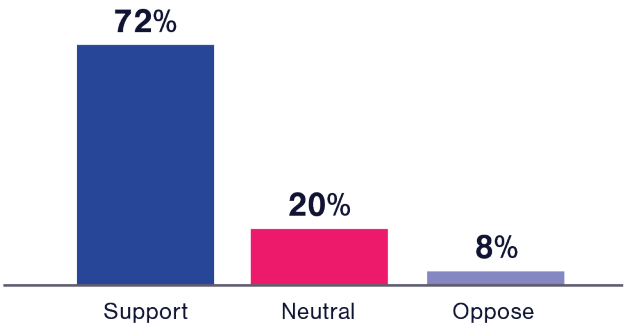
Worried about Hacking of Personal Financial Data (By Residential Area)



SOURCE: CivicScience Consumer Data Privacy Concerns, Question 1.

A strong consensus exists among Americans for a single, nationwide online data privacy law. The CivicScience survey shows that support for a single, nationwide online data privacy law is held by Millennials, Generation Xers, and Baby Boomers, as well as Americans of all ethnicities (Whites, Blacks, Hispanics, and those reporting Other). Likewise, support for a single, nationwide online data privacy law is strong among Americans living in Rural Areas, the Suburbs, and in Cities. While the CivicScience survey shows that 72% of Americans believe there should be a "single, national policy addressing consumer data privacy rules" in the United States, as previously shared, ***opposition to a single, national policy is extremely low – a mere 8% of Americans disagree that there should be a single, national policy.***

Support a Single, National Consumer Data Privacy Policy (Topline Results)



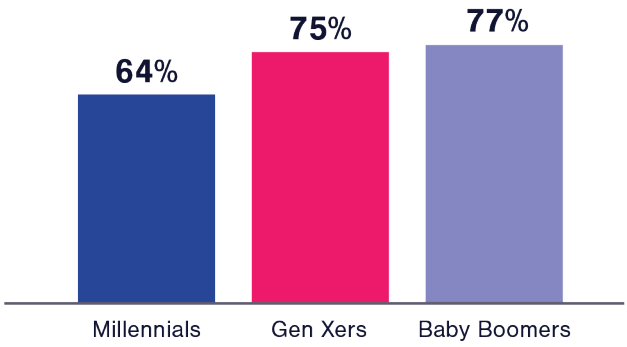
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 4.

A closer examination of the CivicScience privacy survey results supports the analysis that the vast majority of Americans support a single, national online consumer data privacy policy. Nearly two-thirds of Millennials (64%) believe there "should be a single, national policy addressing online consumer data privacy" in the United States. Even larger numbers of older Americans – 77% of Baby Boomers and 75% of Generation Xers – support a single, national online data privacy policy. ***Americans of all ethnicities are in favor of a single, national online data privacy policy*** – 71% of Hispanics, 68% of Blacks, 73% of Whites, and 65% of those reporting Other support a single, national online data privacy policy. Very strong majorities of Americans at all income levels are united in support of a single, national online data privacy policy – 70% of those with annual incomes of under $50,000, 74% of those with annual incomes between $50,000 and $100,000, and 74% of upper-income Americans support a single, national online data privacy policy. And very strong majorities of Americans living in Rural Areas (70%), the Suburbs (73%), and in Cities (73%) support a single, national online data privacy policy.

CivicScience Question 4:

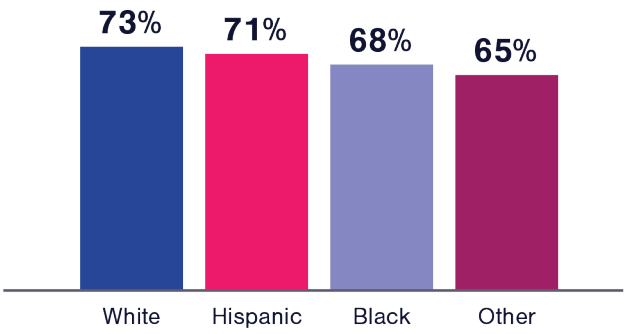
There should be a single, national policy addressing consumer data privacy rules in the United States.

Support a Single, National Consumer Data Privacy Policy (By Generation)



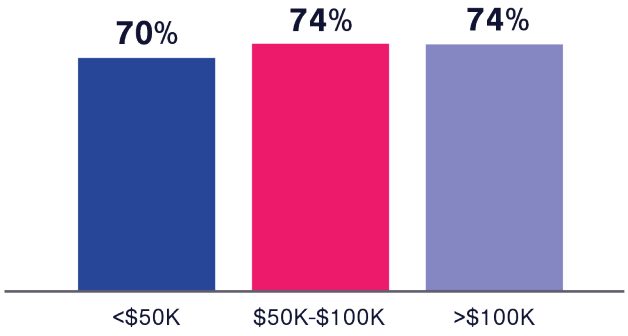
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 4.

Support a Single, National Consumer Data Privacy Policy (By Ethnicity)



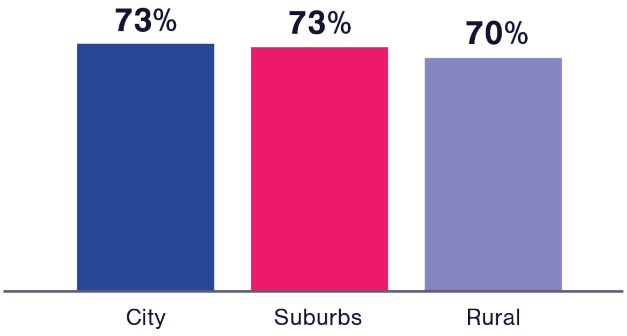
SOURCE: CivicScience Consumer Data Privacy Concerns, Question 4.

Support a Single, National Consumer Data Privacy Policy (By Income)



SOURCE: CivicScience Consumer Data Privacy Concerns, Question 4.

Support a Single, National Consumer Data Privacy Policy (By Residential Area)



SOURCE: CivicScience Consumer Data Privacy Concerns, Question 4.

V. Conclusion

The internet is an important resource for U.S. consumers and is seen by many as essential to daily life, but privacy abuses, data breaches, and misuses of personal information are eroding consumer trust in the internet ecosystem. The CivicScience privacy survey results show that Millennial Americans are concerned both about the exploitation of their personal data and location information and about the possibility of their personal financial information being hacked from the online tech and social media companies they use. These concerns are shared by older Americans and consumers of all ethnicities – Hispanics, Blacks, Whites, and those reporting Other – and they stretch across all geographic areas of the country and all income levels.

There is widespread consensus among U.S. consumers that a "single, national policy addressing consumer data privacy should be adopted in the United States" – and opposition to a single, national policy is extraordinarily low among all segments of the U.S. population. As a result, the Internet Innovation Alliance believes that now is the time for the U.S. Congress to address the concerns of millions of Americans by adopting a single, nationwide framework for safeguarding the online personal privacy of consumers.

In partnership with:

ICONTALKS®
ENTERTAIN. ENGAGE. INSPIRE.

HTTP
Hispanic Technology & Telecommunications Partnership
The National Latino Voice on Technology & Telecommunications

MAP
MILLENNIAL ACTION PROJECT

Appendix A

News Articles Addressing Privacy Abuses & Data Breaches in 2018

The Washington Post, Tony Romm and Craig Timberg, *Google Reveals New Security Bug Affecting more than 52 Million Users* (Dec. 10, 2018).

The Washington Post, Tony Romm, *Facebook Says A New Bug Allowed Apps to Access Private Photos of up to 6.8 Million Users* (Dec. 14, 2018).

Wall Street Journal, Douglas MacMillan and Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public* (Oct. 8, 2018) (describing how a "software glitch" gave potential access to outside developers of consumers' personal information).

BuzzFeed News, Ryan Mac, *Facebook Says A Bug May Have Exposed The Unposted Photos of Millions of Users* (Dec. 14, 2018).

The New York Times, Mike Isaac and Sheera Frenkel, *Facebook Security Breach Exposes the Accounts of 50 Million Users* (Sep. 28, 2018).

Gizmodo, Kashmir Hill, *Facebook Is Giving Advertisers Access to Your Shadow Contact Information* (Sep. 26, 2018); The Mercury News, Levi Sumagaysay, *Facebook targets ads using phone numbers submitted for security purposes* (Sep. 27, 2018). These news outlets reported on the study published by professors from Northeasten University and Princeton University. See Giridhari Venkatadri, Elena Lucherini, Piotr Sapiezynski, and Alan Mislove, *Investigating sources of PII used in Facebook's targeted advertising* (2018).

The New York Times, Niraj Chokshi, *Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation* (May 25, 2018).

CNN, Heather Kelly, *Twitter says all 336 million users should change their passwords* (May 3, 2018).

The Guardian, Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach* (Mar. 17, 2018); The New York Times, Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions* (Mar. 17, 2018).

The New York Times, Vindu Goel and Rachel Adams, *Card Data Stolen From 5 Million Saks and Lord & Taylor Customers* (Apr. 1, 2018) (exposing personal data for 53,000 customers and approximately 19.4 million voters).

The Sacramento Bee, Adam Ashton, *Voter, Bee databases hit with ransomware attack* (Feb. 7, 2018).

Fox Business, Thomas Barrabi, *Panera Bread data breach exposes customer records* (Apr. 2, 2018) (estimating personal information for some 37 million customers disclosed).

Fortune, Glenn Fleishman, Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says (Sep. 8, 2018); see also Government Accountability Office, *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* (Aug. 2018).

Business Insider, Dennis Green and Mary Hanbury, *If you bought anything from these 10 companies last year, your data may have been stolen* (Jan. 24, 2019).

The New York Times, Mike Isaac and Cecilia Kang, *Facebook Expects to Be Fined Up to $5 Billion by F.T.C. Over Privacy Issues* (Apr. 24, 2019).

The New York Times, Mike Isaac, *New York Attorney General to Investigate Facebook Email Collection* (Apr. 25, 2019).

The Wall Street Journal, Sam Schechner, *Facebook Faces 10 Privacy Probes in Ireland as Global Scrutiny Intensifies* (Feb 28, 2019).

The Wall Street Journal, Brent Kendall and John D. McKinnon, *Looming Facebook Fine Points to a Tougher Cop on the Tech Beat* (Apr. 25, 2019).

The Wall Street Journal, Kim Mackrael and Paul Vieira, *Facebook Probe Found Major Shortcomings in Privacy Protection, Canada Privacy Watchdog Says* (Apr. 25, 2019).

TechCrunch, Zack Whittaker, *Facebook hit with three privacy investigations in a single day* (Apr. 25, 2019).