The State of Online Privacy and Data Security

U.S. Senate Committee on Commerce, Science, and Transportation

Ranking Member Maria Cantwell

November 2019

Table of Contents

Executive Summary

In 2018, American consumers spent over $14 billion online on Black Friday and Cyber Monday combined.[1] And the 2019 holiday season promises to be even busier for online retailers, with sales projected to increase 4.5-5% from 2018.[2] More shoppers are expected to shop online this holiday season than ever before, with 59% of consumer holiday spending projected to come from online purchases. This is a 14-18% increase in online sales over the 2018 holiday season.[3]

This holiday season, **59%** of all shopping will be done **online**.

SOURCE: Deloitte

While many online shopping sites and apps give consumers the security and transparency they deserve, as digital shopping increases more and more Americans are concerned about whether their data is protected, how it is used, and to whom it is sold.

Unfortunately, consumers do not have clear rights to protect their data, to stop them from being profiled, or to prevent unwanted data transfers under the law. There is currently no general right to access one's data, and no right to have data deleted or corrected. The existing legal structure to protect Americans' privacy, which is based on general prohibitions against deceptive and unfair practices, does not provide consumers the specific data rights they need in the digital economy.

This report highlights the following five areas of privacy concern for consumers in the digital economy:

1. Data Breaches
2. Who Has My Data?
3. Online Profiling and Targeting
4. Data-Driven Discrimination
5. Internet-Connected Devices

Illegally obtained medical records and passports can sell for **$1,000 or more** on the black market.

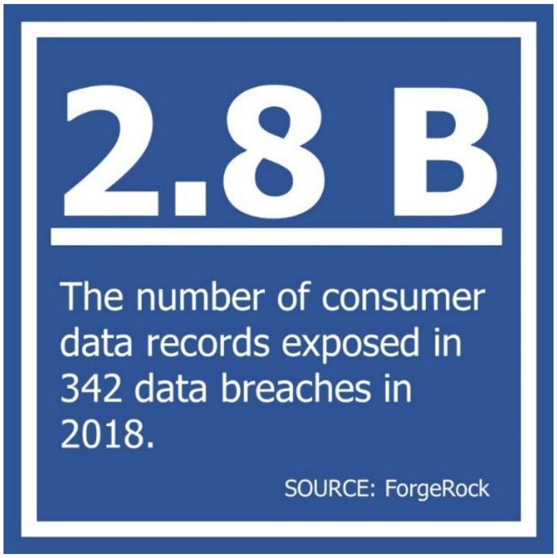
SOURCE: Radware

Data Breaches

Every day, companies face sophisticated threats of cyber-attacks and many are not prepared to defend their systems or do not have the proper controls in place to secure data. In fact, hackers attack consumers every 39 seconds.[4]

In the wrong hands, banking and credit card information, Social Security numbers, mailing address, phone numbers, dates of birth, purchase histories, and other personal information can be used to make fraudulent charges, give credibility to scam artists targeting consumers, expose consumers to spam marketing, and more. In 2017, nearly 17 million Americans were victimized by identity fraud.[5]

Data breaches have become commonplace, and millions of consumers have fallen victim. In 2018, according to one report, more than 2.8 billion consumer data records, including financial, medical, and other personal information, were exposed in 342 separate breaches.[6]



2.8 B

The number of consumer data records exposed in 342 data breaches in 2018.

SOURCE: ForgeRock

These breaches compromise consumer privacy. In 2013, three billion Yahoo accounts were hacked, affecting Yahoo e-mail and other applications. Breaches can expose a wide variety of sensitive data. In fact, 97% of all data breaches target personally-identifiable information, with dates of birth and Social Security numbers being the most common types of information stolen.[7] According to a recent report, health and medical records sell for up to $1,000 on the black market because they contain contact information, a Social Security number, and even payment information.[8] Likewise, passport information can sell for over $1,000 because it can be used to create fake IDs.[9]

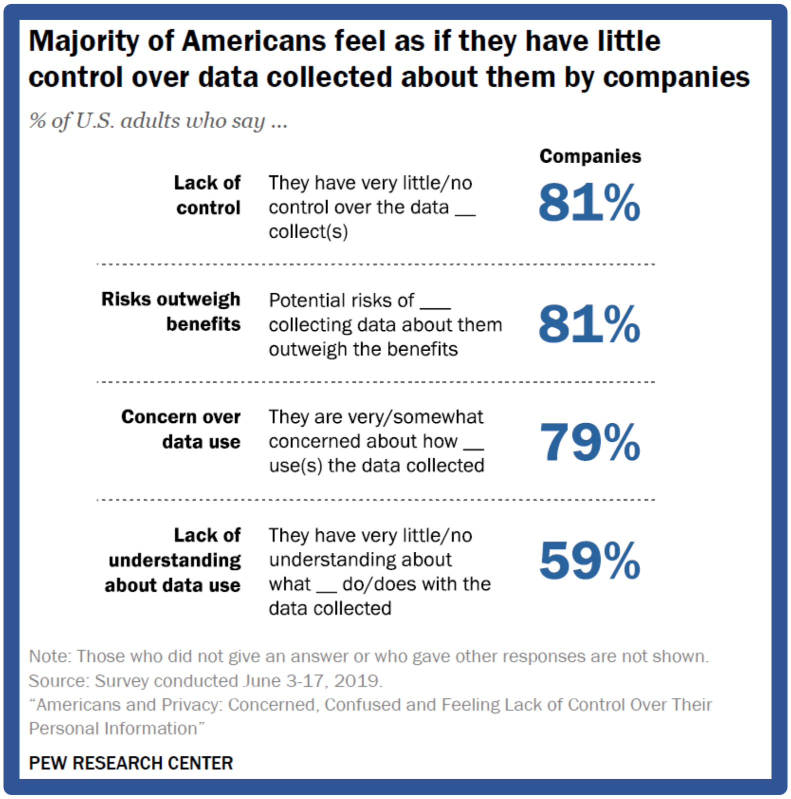
One example is the 2017 Equifax breach, which put the personal data of 148 million Americans at risk. In this breach, names, home addresses, phone numbers, dates of birth, Social Security numbers, and driver's license numbers were compromised. The credit card numbers of approximately 209,000 consumers were also exposed.[10]

Who Has My Data?

Most people do not understand the privacy policies within each app, or at the bottom of nearly every website they visit. Privacy policies are generally complex and hard to read, do not offer clear choices, and fail to explain where consumer data will be transferred or how, exactly, it will be used. In order to gain access to many products and services, people are forced to accept user agreements and terms that strip them of control over their data. This data is then often sold to unknown third parties who use it for a variety of purposes – from targeted advertising to personalized web browsing experiences and more.

Data is collected from a variety of sources: web browsing trackers, social media companies, household electronic appliances, apps, public records, and many others. For example, *Forbes* magazine reported that 70% of mobile apps share data with third parties, and 15% of the apps reviewed were connected to five or more trackers.[11]

Driving this growth is the use of personal data and online browsing habits, everything from precise location information to personal health and biometric information. A recent study found that over 80% of mental health apps shared the data they collected with advertisers, data analytics companies, Facebook, or Google.[12]



Majority of Americans feel as if they have little control over data collected about them by companies

% of U.S. adults who say ...

		Companies
Lack of control	They have very little/no control over the data __ collect(s)	81%
Risks outweigh benefits	Potential risks of ___ collecting data about them outweigh the benefits	81%
Concern over data use	They are very/somewhat concerned about how __ use(s) the data collected	79%
Lack of understanding about data use	They have very little/no understanding about what __ do/does with the data collected	59%

Note: Those who did not give an answer or who gave other responses are not shown.
Source: Survey conducted June 3-17, 2019.
"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

PEW RESEARCH CENTER

Online Profiling and Targeting

As consumers browse the web, interact with social media, or use other online services, they probably see advertisements for items they've previously searched for online (even on another device), purchased in a store, or saw on a nearby billboard. For some consumers, it can feel creepy, invasive, or alarming. Consumers likely would not be surprised to know that the current legal framework does little to prevent companies from collecting or selling the data that enables these advertisements or the online profiles that are created.

72%

of Americans report feeling that all, almost all, or most of what they do online or while using their cellphone is being **tracked by advertisers, technology firms or other companies**

SOURCE: Pew Research

Advertisers and marketers are finding more ways to reach consumers using their personal information and data to target ads specifically to individual users.

The majority of Americans are aware that their digital identity is being tracked, but many are unaware of the extent.[13] For example, smart TVs collect viewing data and may send it to Amazon, Facebook, Doubleclick, Netflix, and others.[14] This data may be used to recommend programming, as well as to target ads directly to consumers. Moving forward, it is expected that advertising will follow people as they walk down the street or drive in their cars – automated billboards communicating with cell phones to collect gender, age, race, income, and spending habit data to update their ads in real time. These ads might also show up on a social media feed or a smart TV at home.[15]

In 2019, for the first time, **digital ad spending** is expected to account for

over 50%

of all media ad spending.

SOURCE: eMarketer

The market for data is lucrative. In the United States, digital ad spending is expected to reach $129 billion and account for over 50% of all media ad spending.[16] Globally, digital ad spending will rise by over 17% in 2019, growing to over $333 billion.[17] By 2023, digital ad spending is forecast to become more than a $500 billion market.[18]

Having honest and transparent ad practices helps both businesses and consumers. Recent research by the Harvard Business Review (HBR) shows that when shoppers know that the advertisements they see are tailored to them, their trust in the retailer increases, which also boosts revenues and increases traffic to the advertisements.[19] Another HBR study found that when consumers are given greater say over what happens with information they've shared with Facebook, the personalized ads were twice as effective.[20]

Data-Driven Discrimination

Credit card offers and credit limits, housing advertisements, and offers of employment, among others, are increasingly being determined by powerful computer instructions, known as algorithms, that process data. Because algorithms often use name, geolocation, zip code, and other proxies for race and socioeconomic status, they can sometimes have a discriminatory impact on marginalized groups.

Discrimination has plagued the United States throughout its history. Practices such as redlining, where banks and other lending institutions refuse to lend to people living in certain areas from qualifying for home loans even though they are otherwise credit-worthy, were pervasive. Unfortunately, these practices have the potential to be even more pernicious in a new, digital form. As more and more data is collected to generate online profiles unknown to consumers, discrimination has the potential to become more targeted and, without proper enforcement, less identifiable.

For instance, in March 2019, Facebook reached a settlement with a number of civil rights organizations over charges that it had allowed advertisers to exclude people of certain races, ages, and genders from seeing ads for housing, job, and credit opportunities – illegal discrimination against historically disenfranchised groups.[21] Without vigilant enforcement, however, people may never know whether they are being discriminated against.

In another example, researchers at Carnegie Mellon University found that Google's advertising platform would sometimes target ads to job seekers based on data about gender. They found that male job seekers were more likely than their female counterparts to be shown ads for high-paying executive jobs.[22]

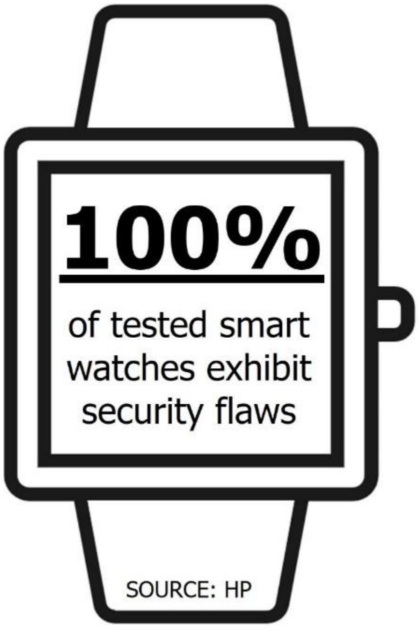
The FTC also found that data brokers would create profiles for consumers who are "underbanked" or "financially challenged" and sell that data to advertisers, resulting in people of lower incomes being shown targeted ads for "subprime loans." Often, Consumers don't know this is happening at all.[23]

> **"Proxies for race,** including name and geo-targeted advertising, **often result in discriminatory employment, advertising and marketing practices."**
>
> **-Brandi Collins-Dexter**
>
> Senior Campaign Director, Color of Change
>
> in testimony to the U.S. House Subcommittee on Consumer Protection and Commerce, February 26, 2019

Internet-Connected Devices

Smart speakers, wearable fitness trackers, internet-enabled toys, home surveillance technology, smart watches, internet-connected cars, and other internet-connected devices – also known as Internet of Things (IoT) – lack adequate privacy and security controls, according to researchers. Any device with a Bluetooth connection set to "discoverable" can be tracked with relative precision.

For example, wearable fitness devices collect data about the user's heart rate, location, and other information. Oftentimes, individuals are not adequately informed about the amount and scope of the data and who has access to it.[24] IoT devices are among the most vulnerable to hackers who know that consumers too often do not reset automatic passwords or understand how best to safeguard their devices.


100%

of tested smart watches exhibit security flaws

SOURCE: HP

The total number of internet-connected devices is expected to reach more than 75 billion worldwide by the year 2020, an increase of more than 500% in a decade.[25] But many of the devices that make up the IoT pose significant privacy and security risks.

70%

of mobile apps share your data with third parties

SOURCE: Forbes

In 2015, a couple in Indianapolis reported their baby monitor had been hacked by someone playing "Every Breath You Take" by The Police and making "sexual noises." Other families have reported similar instances.[26] Similarly, many children's toys contain reported privacy vulnerabilities. The Bluetooth-enabled "My Friend Cayla" doll, for instance, has no mention of privacy on its packaging and its terms of service give little information on what data the toy collects, how the information is used, or where it is sent.[27]

Privacy and security vulnerabilities involving children may be especially scary, but internet-connected devices pose broader risks as well. In a single week, a *Washington Post* reporter found more than 5,400 data trackers on his smart phone – all gathering and distributing data without his knowledge.[28]

Endnotes

[1] Lauren Thomas," Cyber Monday sales break a record, with $7.9 billion spent online, Adobe Analytics" says." *CNBC*. UPDATED WED, NOV 28 2018, Accessed November 21, 2019, https://www.cnbc.com/2018/11/27/cyber-monday-sales-break-record-a-record-7point9-billion-spent-online.html

[2] "Deloitte 2019 holiday retail survey: Top Ten Insights," *Deloitte Insights*, accessed November 21, 2019, https://www2.deloitte.com/content/dam/insights/us/articles/6382_2019-holiday-survey/DI_2019-holiday-survey.pdf?nc=1

[3] Ibid.

[4] Michel Cukier, "Study: Hackers Attack Every 39 Seconds," University of Maryland, February 9, 2007, accessed on November 21, 2019, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

[5] "Strategy & Research Study: Identity Fraud Hits All Time High with 16.7 Million U.S. Victims in 2017, According to New Javelin," *Javelin Strategies*, February 6, 2018, accessed on November 21, 2019, https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin

[6] "U.S. Consumer Data Breach Report, 2019," *ForgeRock*, 2019, accessed 11/21/2019, https://www.forgerock.com/resources/view/92170441/industry-brief/us-

[7] Ibid.

[8] Megan Leonhardt, "Here's How Much Money Hackers Get for Your Social Security Number and Other Info on the Black Market," *CNBC*, August 22, 2018, accessed November 21, 2019, https://www.cnbc.com/2018/08/22/how-much-hackers-get-for-social-security-numbers-on-the-black-market.html

[9] Ibid.

[10] "Equifax Data Breach," *Electronic Privacy Information Center*, accessed November 21, 2019 https://epic.org/privacy/data-breach/equifax/

[11] Lee Matthews, "70% Of Mobile Apps Share Your Data with Third Parties," *Forbes*, June 13, 2017, accessed on November 21, 2019, https://www.forbes.com/sites/leemathews/2017/06/13/70-percent-of-mobile-apps-share-your-data-with-third-parties/#e3a521115692

[12] Jon Fingas, "Mental health apps are sharing data without proper disclosure," *Engadget*, April 20, 2019, accessed on November 21, 2019, https://www.engadget.com/2019/04/20/mental-health-apps-share-data/

[13] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," *Pew Research Center*, November 15, 2019, accessed on November 21, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[14] James K. Willcox, "How to Turn Off Smart TV Snooping Features," *Consumer Reports*, updated September 27, 2019, accessed on November 21, 2019, https://www.consumerreports.org/privacy/how-to-turn-off-smart-tv-snooping-features/

[15] Thomas Germain, "Digital Billboards Are Tracking You. And They Really, Really Want You to See Their Ads," *Consumer Reports*, November 20, 2019, accessed on November 21, 2019, https://www.consumerreports.org/privacy/digital-billboards-are-tracking-you-and-they-want-you-to-see-their-ads/

[16] Jasmine Enberg, "US Digital Ad Spending 2019," *EMarketer,* March 28, 2019, accessed November 21, 2019, https://www.emarketer.com/content/us-digital-ad-spending-2019

[17] Jasmine Enberg, "Global Digital Ad Spending 2019," *EMarketer,* March 28, 2019, accessed November 21, 2019, https://www.emarketer.com/content/global-digital-ad-spending-2019

[18] Ibid.

[19] Leslie K. John, Tami Kim, and Kate Barasz, "Ads That Don't Overstep," *Harvard Business Review*, January-February 2018 Issue, accessed on November 21, 2019, https://hbr.org/2018/01/ads-that-dont-overstep

[20] Ibid.

[21] Emily Dreyfuss, "Facebook Changes Its Ad Tech to Stop Discrimination," *Wired,* March 19, 2019, accessed on November 21, 2019, https://www.wired.com/story/facebook-advertising-discrimination-settlement/

[22] Tom Simonite, "Probing the Dark Side of Google's Ad-Targeting System," *MIT Technology Review*, July 6, 2015, accessed on November 21, 2019, https://www.technologyreview.com/s/539021/probing-the-dark-side-of-googles-ad-targeting-system/

[23] "Data Brokers: A Call for Transparency and Accountability," *Federal Trade Commission*, May 2014, accessed on November 21, 2019, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[24] Steven Spann, "Wearable Fitness Devices: Personal Health Data Privacy in Washington State," *39 Seattle U. L. REV. 1411 (2016)*, accessed on November 21, 2019.

[25] "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," *Statista*, accessed on November 21, 2019, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[26] Charlie De Mar, "Baby monitor hacker sends a frightening message to Indianapolis family," *Fox59*, Updated October 1, 2015, accessed on November 21, 2019, https://fox59.com/2015/08/27/baby-monitor-hacker-sends-a-frightening-message-to-indianapolis-family/

[27] Katie McInnis, David Butler, and Kara Kelber, "Internet-Connected Toys Are Spying on Kids, Threatening Their Privacy and Security," Consumer Reports, December 6, 2016, accessed on November 2019, https://advocacy.consumerreports.org/press_release/internet-connected-toys-are-spying-on-kids-threatening-their-privacy-and-security/

[28] Geoffrey Fowler, "It's the middle of the night. Do you know who your iPhone is talking to?" *The Washington Post*, May 28, 2019, Accessed November 21, 2019, https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/