consumeraction

Location Tracking and Data Collection:

Who's tracking U.S. consumers, how much control do they have over their location privacy, and what laws currently protect their consumer rights?

May 2019

About Consumer Action

Consumer Action is a non-profit organization that has championed the rights of underrepresented consumers nationwide since 1971. Throughout its history, the organization has dedicated its resources to promoting financial and consumer literacy and advocating for consumer rights both in the media and before lawmakers to promote economic justice for all. With the resources and infrastructure to reach millions of consumers, Consumer Action is one of the most recognized, effective and trusted consumer organizations in the nation.

Consumer education. To empower consumers to assert their rights in the marketplace, Consumer Action provides a range of educational resources. The organization's extensive library of free publications offers in-depth information on many topics related to personal money management, housing, insurance and privacy, while its hotline provides non-legal advice and referrals. At Consumer-Action.org, visitors have instant access to important consumer news, downloadable materials, an online "help desk," the Take Action advocacy database, and more. Consumer Action also publishes unbiased surveys of financial and consumer services that expose excessive prices and anti-consumer practices to help consumers make informed buying choices and elicit change from big business. Our in-language media outreach allows us to share scam alerts and other timely consumer news with a wide non-English-speaking audience.

Community outreach. With a special focus on serving low- and moderate-income and limited-English-speaking consumers, Consumer Action maintains strong ties to a national network of nearly 7,000 community-based organizations. Outreach services include training and bulk mailings of financial and consumer education materials in many languages, including English, Spanish, Chinese, Korean and Vietnamese. Consumer Action's network is the largest and most diverse of its kind.

Advocacy. Consumer Action is deeply committed to ensuring that underrepresented consumers are represented in the national media and in front of lawmakers. The organization promotes pro-consumer policy, regulation and legislation by taking positions on dozens of bills at the state and national levels and submitting comments and testimony on a host of consumer protection issues. Additionally, its diverse staff provides the media with expert commentary on key consumer issues supported by solid data and victim testimony.

www.consumer-action.org

Table of Contents

Introduction

Individuals today lack control over the collection and use of their personal data, despite growing agreement that data privacy regulation is needed to set clear guidelines over how our data is collected, retained and treated. Mostly, our personal data is shared and sold for the benefit of advertisers and marketers. However, without adequate controls placed on giant online advertisers like Google and Facebook, they are free to collect massive amounts of data and create personal user profiles based on our online activities. This includes almost everything we do online, from social media interactions and web searches to purchases and the location of our connected devices.

This paper focuses on the collection and use of geolocation data for a variety of industries. We examine *who* has access to our location data, *how* the data is used, and *whether* our location is shared with third parties, and for what purposes. We consider the benefits and drawbacks to the collection and sharing of location data, and consider the fairness of today's notice and consent regime and whether we really understand the tradeoffs.

We examine location data use by:

- Internet service providers;
- Social media companies;
- Vehicles;
- Food delivery companies;
- "Wearable" technologies (fitness and health apps); and
- Employers.

Individuals' opinions about the use of their location information are influenced by who is accessing the data and for what reasons. We might have different tolerance levels for location access by an app developer than we would for law enforcement. Some of us may be comfortable with online companies knowing our location for a particular purpose, but uncomfortable when they share our location history with others.

Countless ways to track your location

On any given day, consider how many ways our location is being tracked—sometimes with our knowledge and consent, and sometimes without it. We can be tracked via our smartphones, mobile apps, internet service providers and connected home devices. Microchips (in our payment cards) and radio-frequency identification (RFID) tags (such as are found in toll payment devices) also may provide location data when close to a reader. It's possible to track consumers when they're engaging in the most routine activities of daily life: carrying their phones, spending time at home ("Alexa, turn on the lights") or driving their cars. But people might not know that companies track customers' location when they visit stores or malls in order to analyze traffic and customize marketing. Using location data, retailers can entice consumers with a targeted ad, discount or special offer.

Some retailers use location data for dynamic pricing—price adjustments based on a customer's proximity to their store or a competitor's store, or whether the consumer is shopping online. Earlier this year it was reported that Target's mobile app hiked the price of a television (from $499 to $599) as a shopper pulled into the store's parking lot. KARE-TV's investigation revealed that four of the 10 items they shopped for jumped up in price when they entered the store.[1] Target requests access to users' location when they download the app, in order to provide "nearest store" information, offer coupons and, it appears, customize pricing.

Some firms are using location information to better understand consumer behavior. The *New York Times* quoted a marketing expert's example of how location tracking could reveal that a consumer frequents fast food restaurants despite searching online for healthy recipes. "We look to understand who a person is, based on where they've been and where they're going, in order to influence what they're going to do next," she explained. The same article noted that some financial firms buy and use location data related to a company's employees, facilities and customers to make investment decisions before that company reports earnings.[2]

Many mobile apps and websites track users' location even when there is no reason for collecting the information (i.e., the user's location isn't needed for the app to function). Many questioned why a smartphone "flashlight" app or the Dictionary.com website needs to track one's location.[3]

In 2018, the mobile data analysis firm MightySignal found that 1,200 apps in the Google Play Store and 200 in the Apple App Store had location sharing capabilities.[4]

Some applications like Snap Map allow linked Snapchat users to access the location of other users. Other apps, like Spyzie, will track the whereabouts of "contacts" on your mobile phone.[5] Some parents are using an app called MomIAmOk to check in with kids and to confirm their location.[6] If a child doesn't respond to the check-in, the app can

---

[1] "The Target app price switch: What you need to know." Chris Hrapsky. KARE-TV. Updated Feb. 6, 2019. https://www.kare11.com/article/money/consumer/the-target-app-price-switch-what-you-need-to-know/89-9ef4106a-895d-4522-8a00-c15cff0a0514

[2] "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller and Aaron Krolik. New York Times. Dec. 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[3] "A shock in the dark: Flashlight app tracks your location." Bob Sullivan. NBCNews. Jan. 16, 2013. https://www.nbcnews.com/technolog/shock-dark-flashlight-app-tracks-your-location-1B7991120

[4] "Your apps are tracking you—here's how to stop them." Kari Paul. MarketWatch. Dec. 16, 2018. https://www.marketwatch.com/story/your-apps-are-tracking-you-heres-how-to-stop-them-2018-12-11

[5] "7 Ways to Track A Cell Phone Location for Free." Steve Chen. Spyzie. Jan. 2, 2019. https://www.spyzie.com/mobile-tracker/tracking-phone-location-free.html

[6] MomIAmOk website. Viewed on March 1, 2019. http://www.momiamok.com/

determine the young person's whereabouts and provide that information to parents or police.[7]

Companies that offer roadside assistance use location to help drivers when their car breaks down. If you own a "smart" car, your location can be tracked using a roadside assistance system built into the car. Banks may access a mobile phone's location to fight fraudulent transactions.[8] Fitness trackers like Fitbit have helped police solve murders and other crimes using location data.[9]

In the last two years, Google has been served with police warrants to identify phones that were near the scene of a serious crime. In doing so, these virtual "dragnets" could gather the location data of innocent people who were at or near the scene.

U.S. Immigration and Customs Enforcement (ICE) agents are accessing driver location information through a private, national database of license plate numbers to track down undocumented immigrants, according to the American Civil Liberties Union (ACLU).[10] The database is chock-full of vehicle location records from cameras that clock speed limits and snap license plate photos at toll plazas. The ACLU found that scanners log the time, location and license plate data of *all* cars that pass by. According to the *Washington Post*, while GPS tracking requires police to get a warrant, immigration enforcement agents and local police can access years of location data without a judge's permission.[11]

Google's Android phones track users' location through history settings as well as web and activity settings. A 2018 Associated Press (AP) investigation found that Google continued to collect users' location data even when those features were turned off or paused. AP reported that Google stores users' location when they use its map app. Some Google searches, such as "kids science kits" and "chocolate chip cookies," pinpoint users' precise location and *save* it in their Google account, according to AP's investigation.[12]

---

[7] "They put microchips in their employees. Now this company is helping parents track their children." Peter Holley. Washington Post. Sept. 19, 2018. https://www.washingtonpost.com/technology/2018/09/19/they-put-microchips-their-employees-now-this-company-is-helping-parents-track-their-children/

[8] Letter from AT&T to Senator Wyden. June 15, 2018. https://www.wyden.senate.gov/imo/media/doc/at&t%20letter%20to%20RW%206.15.pdf

[9] "Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing." Christine Hauser. New York Times. Oct. 3, 2018. https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html

[10] "Documents Reveal ICE Using Driver Location Data From Local Police for Deportations." Vasudha Talla. ACLU Northern California. March 13, 2019. https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data

[11] "ICE is tapping into a huge license-plate database, ACLU says, raising new privacy concerns about surveillance." Drew Harwell and Tony Romm. Washington Post. March 13, 2019. https://www.washingtonpost.com/technology/2019/03/13/ice-is-tapping-into-huge-license-plate-database-aclu-says-raising-new-privacy-concerns-about-surveillance

[12] "Google tracks your movements, like it or not." Ryan Nakashima. AP News. Aug. 13, 2018. https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb

Employers track employees' location by mobile phone and computer—in some cases for legitimate business purposes (such as to bill clients), but sometimes even during non-working hours.

Location access without consent

For map apps, rideshare services like Uber and Lyft, and food delivery services, users have to share their location for functionality's sake. But what often is not disclosed to users—or is buried in fine print—is that location information is shared or sold to other companies. For instance, some weather apps may request a user's general location to provide a more precise forecast or post weather alerts, but users, in most cases, wouldn't know or understand that the app is selling data about their location history.

According to a *New York Times* investigation, "At least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information. Several of those businesses claim to track up to 200 million mobile devices in the United States."[13]

In 2018, the *New York Times* mapped out the location tracking abilities of apps and discovered how invasive this tracking can be. When the *Times* tracked a volunteer, with her permission, the data revealed exactly where she went. "The app tracked her as she went to a Weight Watchers meeting and to her dermatologist's office for a minor procedure. It followed her hiking with her dog and staying at her ex-boyfriend's home, information she found disturbing."[14]

While location data is often aggregated and anonymized and doesn't identify individual users, it can be linked to other data sources to identify specific individuals, according to *New York Times* analysis. It has been shown by technologists that online and offline data can be combined to "re-identify" individuals and place them at specific locations based on their phone's whereabouts.

Many consumers are sensitive to having their location data sold or shared with third parties. Knowing the whereabouts of survivors of sexual or physical/domestic abuse presents a real risk to their safety. Conversely, location is crucial to personal safety apps that connect abuse victims to help in case of emergency.

According to an investigation by *Motherboard*, cell phone carriers have sold individuals' location data to data brokers, who then resell this information to all sorts of companies, including bail bondsmen and bounty hunters.[15] Bounty hunters have accessed AT&T, Sprint and T-Mobile customer data intended to allow 911 operators to locate callers in

---

[13] "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller and Aaron Krolik. New York Times. Dec. 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[14] Ibid. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[15] "I Gave a Bounty Hunter $300. Then He Located Our Phone." Joseph Cox. Motherboard. Jan. 8, 2019. https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

emergency situations.[16] Federal Communications Commission (FCC) rules prohibit the sale of precise or "assisted GPS" data to third parties without the phone customer's consent.[17]

"When people in trouble use a wireless phone to call 911, they want to know that first responders can find them no matter where they are—but 'first responders' does not include bounty hunters, debt collectors or stalkers who scam information from carriers by pretending to be police," said privacy advocate Harold Feld of Public Knowledge.[18]

The FCC is studying how to ensure that location information is protected, while making it more precise for first responders.

Google collects location data from Android users' Chrome browser up to 14 times per hour, according to a 2018 study by Vanderbilt University professor Douglas Schmidt. "A major part of Google's data collection occurs while a user is not directly engaged with any of its products." In a 24-hour period, Schmidt says, two-thirds of the data collected was *not* authorized by the user.[19]

According to the *New York Times*, apps can collect and share or sell location data if they disclose the uses in their privacy policy. Consumers rarely read the dauntingly dense legalese, and may be ignorant to what's being done, including that some companies delete location data after using it for advertising purposes, while others retain it for years.

Some legislators have proposed outlawing the collection and sale of personal data.[20]

Consumers' location access preferences

Consumer Action conducted an online survey asking people their opinions on location tracking. Respondents were asked about their main data location collection concerns and how much control they want over the collection and use of personal location data. Respondents overwhelmingly (83%) opposed companies sharing or selling user location data to third parties. Respondents also strongly opposed companies storing their location data after a location-based service, such as a rideshare or directions, was completed.

---

[16] Ibid.
[17] "Telecom Giants Broke the Law By Selling Detailed Location Data. Will They Face Consequences?" Dylan Gilbert. Public Knowledge. Feb. 8, 2019. https://www.publicknowledge.org/news-blog/blogs/telecom-giants-broke-the-law-by-selling-detailed-location-data-will-they-face-consequences
[18] "Public Knowledge Commends FCC for Addressing Consumer Privacy in E911 FNPRM." Shiva Stella. Public Knowledge. March 15, 2019. https://www.publicknowledge.org/press-release/public-knowledge-commends-fcc-for-addressing-consumer-privacy-in-e911-fnprm
[19] "Don't want Google tracking you? You have almost no choice, according to a study." Hayley Tsukayama. Washington Post. Aug. 21, 2018. https://www.washingtonpost.com/technology/2018/08/22/dont-want-google-tracking-you-you-have-almost-no-choice-according-new-study/
[20] "The Consumer Data Protection Act of 2018 Discussion Draft—Senator Wyden." Nov. 1, 2018. https://www.wyden.senate.gov/imo/media/doc/Wyden Privacy Bill one pager Nov 1.pdf

A 2018 study by the Advertising Research Foundation (ARF) trade group concluded that "consumers are willing to share a variety of data regarding who they are, but not information that can be used to personally identify them or locate them in the physical world, even if it would enhance customization of their content experience."

Data control

Consumer Action finds that consumers have little control to limit—or deny—the use of personal location information. A robust national data protection law that would act as a foundation to strengthen individuals' control is needed.

For now, we call on state and local regulators to step up enforcement and fines for companies that violate our limited protections. In February, the Federal Trade Commission (FTC) imposed a record-setting fine on video app TikTok for violating the Children's Online Privacy Protection Act (COPPA) by revealing child users' location.

The more that is revealed about the reach of, and actual and potential harm caused by, location tracking, the more apparent it becomes that we need new consumer rights to prevent businesses from sharing and selling location information.

Location tracking by category

Tracking users' location has become an alarmingly pervasive practice. However, there are certain types of industries, products or services where the practice has become outright commonplace despite a lack of consumer knowledge or control, the real potential for consumer harm, and little or no legal guidelines or regulatory oversight. Consumer Action focused its research on six specific categories—internet service providers, social media, vehicles, food delivery apps, internet-enabled "wearables" and employee tracking—where location tracking either affects a very large population, poses particularly significant privacy risks or may go unrecognized by users.

Internet service providers (ISPs)

The nation's top broadband internet service providers (ISPs)—Comcast, Charter, AT&T and Verizon—allow modern cell phones access to the internet at all times. Users' cell phones act like personal trackers, collecting very accurate accounts of individuals' location (within a few feet to a few hundred meters). What may not be so clear is that each of us gives implicit permission for ISPs to collect all sorts of data on us—just by signing a cell phone contract (with location tracking terms usually buried in the fine print).

When people connect to the internet over a Wi-Fi connection, an ISP can pinpoint their location based on the unique IP address of the router their devices are connected to, whether in a private home or at a coffee shop. When users are connecting to the internet via their mobile phone carrier's network, their private IP addresses are constantly and automatically connecting them to the nearest cell phone tower, which identifies their approximate location. The ISP also collects location metadata (or data

about data), which reveals reams of information, including where a FaceTime call or a text originated from, or what cell phone towers a user is located near at the beginning and end of a call (even when the user is not connected to the internet).

ISP use of location data

Much of the information is combined with other user data. Companies say the data helps them improve their services, learn about trends among certain populations and more efficiently target individuals with ads appropriate to their location or interests. Unique, personal data has been sold to data brokers, who sell it to others, and it can end up being used in highly questionable ways.

Motherboard, a tech media website, published an article last January exposing how ISPs were selling customer location data to data brokers that were reselling it to third parties like car salesmen, property management companies—*even* stalkers and bounty hunters. *Motherboard's* journalist detailed how he was easily able to pay a bounty hunter $300 to locate a T-Mobile phone on Google Maps. The phone user's location was accurate down to a few hundred meters.[21]

Fifteen members of the U.S. Senate reacted by sending a letter to the FCC and the FTC demanding that the regulators investigate exactly how ISPs and the telecom industry sell our location data to unregulated third-party aggregators.[22] The Senators accused the wireless industry of "blatant disregard" for customers' privacy and called on regulators to determine if wireless carriers and data brokers "knew or should have known" that failing to require consumer consent would result in all sorts of unauthorized parties obtaining users' location data.[23] The lawmakers also demanded that carriers notify consumers as to which companies have obtained their location data.

"As long as they are following their own privacy policies, carriers are largely free to do what they want with the information they obtain, including location information, as long as it's unrelated to a phone call," said Albert Gidari, consulting director of privacy at the Stanford Center for Internet and Society, and a former technology and telecommunications lawyer.

In May 2018, *Krebs On Security* revealed how a third-party aggregator, LocationSmart—a service that allowed cell phone users to "find their phone" based on only a phone number, name and other public information—suffered from a vulnerability that allowed just about anyone to find *any* AT&T or Verizon phone in the U.S. to an accuracy of within a few hundred yards. LocationSmart would ping the cell phone towers nearest to the phone being queried and text the person who had input the query into their service, providing the longitude and latitude of the phone. This information

[21] "I Gave a Bounty Hunter $300. Then He Located Our Phone." Joseph Cox. Motherboard. Jan. 8, 2019. https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

[22] Letter from U.S. Senate members to the FTC and FCC. Jan. 24, 2019. https://www.wyden.senate.gov/imo/media/doc/15-senators-location-aggregator-letter-to-fcc-ftc-final.pdf

[23] Ibid.

could then be entered into Google Maps. One computer scientist was even able to track a friend's *directional* movement by prompting LocationSmart to continue to ping a friend's phone over time, according to *Krebs*.[24]

LocationSmart told the *New York Times* that it had bought access to user location data from *all* the major American cell phone carriers. LocationSmart then resold the data. The *Times* article "Service Meant to Monitor Inmates' Calls Could Track You, Too" reveals that the surveillance company Securus sells mobile phone tracking services used predominantly to monitor the origin of inmate phone calls, and can track almost any cell phone "within seconds." Securus got its cell phone location data from a company called 3Cinteractive, which got it from LocationSmart. Securus's services have been used to track a judge, police officers, a drug rehab patient, a missing Alzheimer's patient and a murder suspect, in some cases without a warrant. While Securus has stated that it requires customers to upload a warrant or affidavit and certify that they are authorized to make a surveillance request, it admitted to not verifying these documents.

While some may argue that there are benefits to tracking certain populations (like an Alzheimer's patient or the subject of a search-and-rescue effort), there seem to be more drawbacks than benefits to consumer privacy, particularly when third parties get in on the surveillance game. Although a warrant would likely be required to track an individual, it's chilling to consider how law enforcement or the government could abuse data location technology en masse to monitor the activities of a political group in conflict with the government—even those engaged in lawful protests.

Yet courts are split on the need for a warrant for location data. States differ on whether law enforcement must prove probable cause to gain access to historical cell phone data, or if probable cause is *only* needed to access real-time cell phone data (i.e., movement as it's occurring). The ACLU keeps a list of state cell phone location tracking laws pertaining to law enforcement using cell site location information (CSLI) to track targets.[25]

Meanwhile, a landmark 2018 Supreme Court decision held that consumers *do* have the right to be secure from "unreasonable searches and seizures," even when it comes to their cell phone data, and that federal law enforcement would need a warrant to obtain and search a consumer's CSLI.

Except for media exposés, consumers are largely unaware that their location data is being shared with third parties. ISP responses to *Krebs*' LocationSmart investigation are telling. An AT&T spokesperson said that AT&T "does not permit the sharing of location information without customer consent or a demand from law enforcement." However, after the *Motherboard* article, AT&T added that even though it said it had halted the

[24] "Tracking Firm LocationSmart Leaked Location Data for Customers of All Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site." Krebs on Security. May 17, 2018. https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/

[25] "Cell Phone Location Tracking Laws by State." ACLU. Viewed on March 1, 2019. https://www.aclu.org/issues/privacy-technology/location-tracking/cell-phone-location-tracking-laws-state

practice of aggregating customer locations, it had continued to maintain "some [location services] that protect our customers, such as roadside assistance and fraud prevention." AT&T added that: "In light of recent reports about the misuse of location services, we have decided to eliminate *all* location aggregation services—even those with clear consumer benefits."[26]

Disclosures to customers

If consumers scour ISP privacy policies, they might at least gain a general understanding that their location data will be used and shared with other companies.

All of the wireless carriers analyzed mention pre-loaded phone apps', third parties' and advertisers' use of the location-based data as information potentially collected from customers' devices.

To its credit, AT&T's privacy policy offered more specifics and in easier-to-understand terms than the policies of the other big ISPs. The company outlines the location data that it typically collects: "where your wireless device is located, as well as your ZIP code and street address." It gave an example of a customer dialing 411 and automatically receiving the location of a nearby business without having to input a ZIP code.[27]

AT&T directs users to a webpage where customers can specifically opt out of having their personal information—called Customer Proprietary Network Information (CPNI)—shared with *marketers*.[28] Customer location data falls under CPNI. When sharing CPNI with third parties, AT&T states that it does so with its "family of companies" and with "authorized" law enforcement agents. It may also share cell phone location data with third parties in certain situations, and gives as an example to prevent fraud during a banking transaction. Customers can opt out of this service.[29]

Verizon says it "permits advertisers on our sites, apps and services to place ads based on certain information we have about your Verizon products and services as well as geographic and demographic data," but adds that "information used for this purpose does not identify you individually." When companies like Verizon, AT&T and others say this, they are typically referring to the rules that govern them as telecom companies, since there are no laws governing ISPs' use of personal customer information, or CPNI.

Comcast Xfinity's privacy policy for mobile phones states that any "usage data"—including location information—provided by Comcast to third parties must be kept "confidential" per a contract with the company. Also, like Verizon, Comcast points to the federal law concerning CPNI, and states that the law protects customer data. But again,

---

[26] AT&T is cutting off all location-data sharing ties in March." Alfred Ng. CNET. Jan. 11, 2019. https://www.cnet.com/news/at-t-is-cutting-off-all-location-data-sharing-ties-by-march/

[27] "AT&T Privacy Policy." Viewed on March 1, 2019. https://about.att.com/sites/privacy_policy/full_privacy_policy

[28] "AT&T Customer Proprietary Network Information (CPNI) Restriction Request." Viewed on March 1, 2019. https://www.att.com/ecpnioptout/InitiateCPNIForm.action

[29] "AT&T Manage your privacy choices online form." Viewed on March 1, 2019. http://www.att.com/cmpchoice

this law does not apply to Comcast as an ISP, only as a telecom company, and, like Verizon, Comcast operates as both.

What companies reveal about tracking

ISPs can track consumers with amazing accuracy. Charter's policy (like Verizon's and others') vaguely outlines that it can collect city or ZIP code information (correlated from your phone, modem or router's IP—internet protocol—address) or "geolocation data that indicates where you are at a specific point in time."

AT&T explains that the accuracy of its location tracking "depends on the technology we're using. For example, we can locate your device based on the cell tower that's serving you. The range could be up to 1,000 meters in any direction from the tower in urban areas, and up to 10,000 meters in rural areas. Wi-Fi networks provide more accurate location information, associating you with the place where the network is located—like a coffee shop—or to an area within or around that place. Services such as 411, 911, a "friend locator" application or a navigation/mapping application, require more precise information. So for those we develop a more precise estimate of location by associating the serving cell tower ID with other information, like the latitude and longitude of the tower, radio frequency parameters, GPS information and timing differences in radio signals. Depending on a variety of factors, those methods may estimate the location of your device to within 30 to 1,000 meters."[30]

All of the ISPs state that they do not *sell* customer information; instead they *share* it, and make money on the data through advertising deals. For example, a fast food chain like McDonald's would pay Comcast to advertise to a certain population based on data the ISP had collected—targeting people who have expressed an interest in McDonald's by going to its website or an app for coupon deals, for instance.

Consumer Action found that all of the major ISP privacy policies allowed access to users' location data for selective third parties with some form of consent. Verizon, like the other ISPs, outlined how they may share customer data with "outside companies" when the customer "authorizes" it. Verizon says that, without the consent of the person whose information will be shared, it does not "sell, license or share information" that "individually identifies" users with companies that are not part of its "family of companies" *if* those companies "are not performing work on Verizon's behalf."[31]

It should be noted that customer authorization is almost always in the fine print of an ISP or telecom company contract, or presented as terms or conditions that *must* be accepted in order for a consumer to receive the desired phone account or related service.

---

[30] "AT&T Privacy Policy FAQ." Viewed on March 1, 2019. https://about.att.com/sites/privacy_policy/terms#location

[31] "Verizon Full Privacy Policy." Viewed on March 1, 2019. https://www.verizon.com/about/privacy/full-privacy-policy

CTIA, the international association for the wireless telecommunications industry, stresses that cell phone users should be "meaningfully" notified of how their location data will be collected and used, and that they should consent to the use or disclosure of location data.[32] CTIA's suggested guidelines apply to cell phone carriers, not ISPs, which may be difficult for consumers to parse since some of these companies operate as both.

In April 2017, President Trump's FCC nullified a groundbreaking agency privacy rule[33] that would have treated ISPs like telecom companies with regard to CPNI and privacy.[34] The law was set to go into effect later that year. The rule would have forbidden ISPs from collecting, storing, sharing and selling certain types of customer information—including customer location details—without customers' explicit consent. The rule covered "advertising purposes" as well, meaning the ISPs would *not* have been able to use this "business activity" as a loophole.

Some companies, such as Charter, appear to be advocating for privacy laws despite the administration's lax treatment of the ISP and telecom industry. Charter says "Internet users should have 'opt-in' protections, meaning all entities [including ISPs] must receive opt-in consent to collect and share their [users'] data for purposes other than the actual service they [users] engaged in. Additionally all online entities must be transparent about their information collection and sharing practices by providing concise, easy-to-find, understandable privacy notices to consumers."[35]

Social media

The social media sites and apps we use daily on our mobile phones make money by tracking our every move. If these apps are free to download, users are guaranteed to be paying with their privacy. While this trade-off is widely known, it might be surprising to learn how frequently our location is collected, and that location tracking can go on even when we're not logged in to accounts. Is the privacy price of location tracking worth the services received?

A *New York Times* investigation found that as many as 75 companies received location-tracking data from hundreds of popular apps.[36] The data that reporters identified was incredibly precise—monitoring a mobile phone user's daily travels within a few yards of

[32] "Best Practices and Guidelines for Location-Based Services." CTIA. March 23, 2010. http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf
[33] "Trump has signed repeal of the FCC privacy rules. Here's what happens next." Brian Fung. Washington Post. April 4, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/
[34] "Beyond Net Neutrality: The Importance of Title II for Broadband." Yosef Getachew. Public Knowledge. May 2, 2017. https://www.publicknowledge.org/news-blog/blogs/beyond-net-neutrality-the-importance-of-title-ii-for-broadband
[35] "Charter Urges Congress to Pass Legislation Protecting Privacy Everywhere on the Internet." Tom Rutledge. Charter Communications. April 8, 2018. https://policy.charter.com/blog/charter-urges-congress-pass-legislation-protecting-privacy-everywhere-internet/
[36] "Your apps know where you were last night and they're not keeping it secret." Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik. New York Times. Dec. 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

their whereabouts, sometimes updating their location more than 14,000 times in a single day.[37] In turn, the location data is sold to advertisers, stores, data brokers and investment firms that use the information to learn more about consumer behavior and demographics, and to target individuals with ads.

Once third parties have information that's collected from users' mobile apps, they are able to capture data from associated devices, like a router, laptop or smart TV, and use it to build an even more precise profile associated with an "anonymous" ID number. These third-party companies claim that the data they receive is fully anonymized and de-identified, but the *Times* points out that it's possible to link real names with the location coordinates. For example, if user #923 were tracked to the same address every evening and the same address during the day, it's likely that #923's name could be found with the help of a search engine or commercial datasets. The owners of weather, transit, travel, shopping and dating apps sell this information about users' location.[38]

iPhones allow users to limit location tracking in the phone's privacy settings under "Location Services." iPhone users can choose to "Never" share their location with an app, or only share their location while the app is in use. Android phones used to provide an all-or-nothing approach to managing location tracking, but after a recent update this spring, users can now manage app-level location tracking permissions by reviewing the apps that are tracking the user's location in the phone's settings under "Security and Location."[39]

Google

As the world's largest search engine and digital advertising company, Google's data collection machine is difficult to evade. A 2018 Norwegian Consumer Council investigation dove deep into Google's data collection practices and found a granular tracking design on Android phones that manipulates users into enabling, and thus allowing the tracking of, location history and web and app activity through repeated nudging and hidden default settings.[40]

A Vanderbilt University study also discovered extensive Android data sharing. Vanderbilt computer science professor Douglas C. Schmidt found that an idle Android phone running Google's Chrome browser sent location data back to Google "340 times during a 24-hour period, or at an average of 14 data communications per hour."[41] In

---

[37] Ibid.
[38] "How to stop apps from tracking you." Jennifer Valentino-DeVries and Natasha Singer. New York Times. Dec. 10, 2018. https://www.nytimes.com/2018/12/10/technology/prevent-location-data-sharing.html
[39] "Android 101: How to stop location tracking." Barbara Krasnoff. The Verge. April 12, 2019. https://www.theverge.com/2019/4/12/18302306/android-101-location-tracking-stop-how-to
[40] "Every step you take: How deceptive design lets Google track users 24/7." Norwegian Consumer Council (NCC). November 2018. https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf
[41] "Google data collection research." Douglas C. Schmidt. Digital Context Next. Aug. 21, 2018. https://digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/

comparison, on an Apple iPhone (via its Safari browser), Google was blocked from data collection unless the user was interacting with the iPhone.

Most disturbing were the results of two investigations in 2018 that revealed that Google was tracking users' location even when phone tracking features were disabled. An Associated Press investigation[42] found that location data was being captured from both Android and iPhones that had Google products installed (Google Search, Google Maps, YouTube, Gmail, etc.) even when users had turned *off* location tracking on their devices, and even when location data was not relevant to the Google product.

"Google stores a snapshot of where you are when you merely open its Maps app. Automatic daily weather updates on Android phones pinpoint roughly where you are. And some searches that have nothing to do with location, like 'chocolate chip cookies,' or 'kids science kits,' pinpoint [one's] precise latitude and longitude—accurate to the square foot—and save it to your Google account," according to AP.

Quartz business news found that even when cell phone users thought they were being diligent about managing their privacy settings, their Android phones had been collecting the addresses of nearby cellular towers and sending that data back to Google, even with location tracking turned off. Quartz uncovered that the phone continued to provide real-time location coordinates for Android users and could not be disabled.[43]

Quartz noted: "While information about a single cell tower can only offer an approximation of where a mobile device actually is, multiple towers can be used to triangulate its location to within about a quarter-mile radius, or to a more exact pinpoint in urban areas."

Google has responded that the cell tower data was used to send "push notifications" (alerts sent to the phone from apps) and improve message speed, but was never stored. Google said that its push notification system is "distinctly separate from location services."[44] The company promised to end the practice of collecting cell tower addresses after the Quartz story broke in 2017. While Google told Quartz that it didn't use the location data it collected from cell towers, it did acknowledge that advertisers are able to target consumers using its location data.

According to Quartz, Google's 2017 privacy policy did not disclose to Android users that it collected location data even when the location tracking was disabled on the phone. Now Google's privacy policy says that when a device's location setting is disabled, a user's location is not shared with apps, but the user's IP address is still known.[45]

---

[42] "Google tracks your movements, like it or not." Ryan Nakashima. AP News. Aug. 13, 2018. https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb

[43] "Google collects Android users' location even when location services are disabled." Keith Collins. Quartz. Nov. 21, 2017. https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

[44] Ibid.

[45] "Google privacy policy." Viewed on March 27, 2019. https://support.google.com/accounts/answer/3467281?p=privpol_location&visit_id=636893365196086722-2501801608&rd=1

Last year, the New Mexico attorney general (AG) filed a lawsuit against Google for violating the federal child privacy law by allowing dozens of Android game apps to capture data—including location—about children under the age of 13 without parental consent.[46] The Children's Online Privacy Protection Act (COPPA) is intended to prevent children's personal data from falling into the hands of predators, hackers and over-zealous marketers. According to the AG's complaint, game app developer Tiny Lab collected highly sensitive personal data, including a child's precise location within five meters, and the information was constantly updated.[47] Further analysis by the *New York Times* found that game apps on Android phones and Apple iPhones collected and sent data about users under 13 to third parties, a potential violation of COPPA.[48]

Some gaming app companies exploit a loophole by mislabeling their offerings for "families" (not children) in online app stores. Tech-savvy kids still can access the games, perhaps by stating they are older than 13, which then opens their data to collection. Google eventually barred Tiny Lab from the Google Play store, citing multiple privacy violations.[49]

More recently, the *New York Times* revealed law enforcement's increasing "geofence" requests to Google's Sensorvault database, linked to Google users' location history. In doing so, law enforcement seeks to identify people who were near a crime scene, which has the potential to sweep up innocent bystanders. Google says it only releases users' names and email addresses once detectives narrow down their search to a few mobile devices, and only "where legally required."[50]

Why is Google tracking users' location? The company says it helps improve the "user experience" of its products. Google Maps helps users find the nearest pharmacy or tells them in real-time how long it will take to reach a destination. However, a lot of unnecessary data is being captured as well. Google Search saves logged-in users' search history and takes note of their location even when location isn't needed. Location data is also captured and stored with automatic weather updates on Android phones. The Google Assistant saves users' commands. Video-viewing history is captured on YouTube when users are logged in to their Google accounts. (Users can check (and delete) the location markers Google gathers on their My Activity pages [https://myactivity.google.com/myactivity].)

---

[46] "AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data." New Mexico Attorney General's office. Sept. 12, 2028. https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location__Personal_Data_1.pdf

[47] Ibid.

[48] "How game apps that captivate kids have been collecting their data." Jennifer Valentino-DeVries, Natasha Singer, Aaron Krolik and Michael H. Keller. New York Times. Sept. 12, 2018. https://www.nytimes.com/interactive/2018/09/12/technology/kids-apps-data-privacy-google-twitter.html

[49] Ibid.

[50] "Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works." Jennifer Valentino-DeVries. New York Times. April 13, 2019. https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html

Facebook

If a user has ever given the Facebook app permission to capture location (perhaps when geolocation tagging a vacation photo or post), chances are that user continues to be tracked—even when the app is closed. Paul McDonald, Facebook's engineering director of location infrastructure, noted in a recent blog post[51] that Android users who have allowed location sharing with Facebook have been tracked ever since, even when the Facebook app wasn't in use. McDonald acknowledged that the Android Facebook app had stored a log of users' "precise" location history, but did not define "precise."

Facebook recently rolled out an update allowing Android users to turn off location data collection when they're *not* using Facebook. While app-level location sharing management is new for Android, Apple iPhone users long have had the option to turn off location tracking in the phone's privacy settings. Both iPhone and Android Facebook users can limit their location tracking in the Facebook app's privacy settings, under "Location Services."

A warning for Android users: An Oxford University study reviewed 5,000 of the most popular Android apps and found that 42.5 percent of free apps in the Google Play store would share location and other data with Facebook, making Facebook the second biggest third-party data tracker after Google's parent company Alphabet.[52] This might alarm many who thought they were safe from Facebook's privacy intrusions by not having a Facebook account.

Privacy International, a European-based non-profit, looked closer at the Oxford University study and found that 61 percent of the apps they tested automatically transferred data to Facebook the moment the app is opened—whether or not the user has a Facebook account, and regardless of whether the user is logged into Facebook.[53]

These apps can capture incredibly private and sensitive information. For example, the Period Tracker health app could tell Facebook the exact dates an app user is ovulating, that a user is trying to conceive a child, and for how long she's been trying to conceive. The Kayak travel app could tell Facebook when and where users are booking travel. The BMI Calculator & Weight Loss Tracker might share how overweight a user is, how often he exercises, what he eats and how many steps he takes each day. These are incredibly personal details that could be used to build extremely precise behavioral profiles that are then used to target ads—and who knows what else.

---

[51] "Improving location settings on Android." Paul McDonald. Facebook Newsroom. Feb. 20, 2019. https://newsroom.fb.com/news/2019/02/location-settings-android/

[52] "Third Party Tracking in the Mobile Ecosystem". R. Binns, U. Lyngs, M. Van Kleek, J. Zhao, T. Libert and N. Shadbolt. University of Oxford. Oct. 18, 2018. Page 5. https://ora.ox.ac.uk/objects/uuid:b981733e-a641-4793-be59-12f2b8099a82

[53] "How Apps on Android Share Data with Facebook (even if you don't have a Facebook account)." Privacy International. December 2018. Page 3. https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf

Facebook uses companies it has acquired to help it vacuum up even more user data. In 2014, Facebook bought WhatsApp, once a private messaging app, and started collecting individuals' phone numbers (though the practice was later stopped in Europe because it violates the European Union's strong privacy law).[54] WhatsApp says sharing phone numbers will allow Facebook to make better friend suggestions by matching users' connections across the two apps, and will allow Facebook to show users more relevant ads.[55] Facebook acquired the popular photo-sharing app Instagram in 2012. Last year, news broke that Instagram was testing a feature that would share "Insta" users' location data with Facebook, even when they weren't using Instagram. Researcher Jane Manchun Wong, of TechCrunch, found the feature would allow Facebook to "build and use a history of precise locations."[56] Facebook responded that this data would help the user experience, better tailor ads and improve the product overall. Facebook also noted that the feature was only being tested and may never be widely released. It said that Instagram does not store location history.[57]

Outrage over these practices led Facebook CEO Mark Zuckerberg to do an about-face, recently announcing plans to start shifting messaging channels across Facebook, Instagram and WhatsApp into more intimate and private means of communication—communication that would be confidential and permanently deleted. He wrote in a blog post, "I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever."[58]

Snapchat

In 2017,the mobile message and photo-sharing app Snapchat introduced Snap Map—a real-time world map that lets users see where people are "snapping" (filming and streaming short video clips on the apps). Users can choose whether to share their location with all of their friends, or a select few. When users and their friends allow it, they see their friends' icons or Bitmojis (cartoon avatars) and their location. Users can also check out popular events on the map ("heat maps" of activity show where others are snapping) and view recent public snaps (or videos) that were captured nearby. Location is only shared when the app is open.

While users can go into Ghost Mode and hide their location from the map, those who don't implement that feature may forget—after months of use and no prompts reminding

---

[54] "WhatsApp won't share user data with Facebook in Europe." Chaim Gartenberg. The Verge. March 14, 2018. https://www.theverge.com/2018/3/14/17120446/whatsapp-user-data-sharing-facebook-uk-privacy-ico-protection-gdpr-europe

[55] "Looking ahead for WhatsApp." WhatsApp blog. Aug. 25, 2016. https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp

[56] Jane Manchun Wong. Twitter. Oct. 4, 2018. https://twitter.com/wongmjane/status/1047918370698354689

[57] "Instagram is testing the ability to share your precise location history with Facebook." Jon Porter. The Verge. Oct. 5, 2018. https://www.theverge.com/2018/10/5/17940364/instagram-location-sharing-data-sharing-facebook-test

[58] Mark Zuckerberg. "A Privacy-Focused Vision for Social Networking." Facebook Newsroom. March 6, 2019. https://newsroom.fb.com/news/2019/03/vision-for-social-networking/

them of their location-sharing setting—that the map is constantly updating their location every time they use it. If so, Snapchat "friends" can view unprotected users' every move. The map-tracking feature has also been known to cause drama. Teenagers are the big demographic that use the app, and seeing that one's friends are all hanging out together when not everyone got an invitation to the party can cause hurt feelings. Users who post snaps to the app's public forum called "Our Story" give Snapchat permission to make a snap public on the Snap Map for all Snapchat users to see, meaning that anyone could see where the users are and generally what they are doing. Users' real names are not shared.

Weather apps

Many people start their day by checking the weather, using apps that provide useful reminders to dress appropriately for the day. But free mobile weather apps are notorious for over-sharing: Location data derived from their use is sold to advertisers and data brokers.

The AccuWeather, WeatherBug and Weather Channel apps have been found guilty of selling precise user location data to third parties. AccuWeather was sending precise GPS coordinates and the name and address of users' Wi-Fi routers and Bluetooth connectivity to Reveal Mobile, a data broker. Location data was shared even when iPhone users' location sharing setting was turned off.[59] The *Wall Street Journal* reported that the popular Android app "Weather Forecast—World Weather Accurate Radar" collected users' location data, email addresses and phone numbers and sold it to third parties.[60]

Pokémon GO

The popular game app Pokémon GO took over the world when it launched in 2016, sending millions of users outside to search for Pokémon monsters with their mobile phones. To use the game, Android and iPhone users granted the app access to their location and camera. For Android users, using the app also meant granting access to their USB storage, contacts and network connections.[61] iPhone users shared photos with the app, and if they logged in through their Google accounts, received full access to the game. The game was widely criticized for allowing unnecessary access to all information in users' Google accounts, including Gmail, Google Drive documents, Google Maps location history and Google search and browsing history.[62] Once news

[59] "Advisory: AccuWeather iOS app sends location information to data monetization firm." Will Strafach. Hacker Noon. Aug. 21, 2017. https://hackernoon.com/advisory-accuweather-ios-app-sends-location-information-to-data-monetization-firm-83327c6a4870

[60] "Popular weather app collects too much user data, security experts say." Newley Purnell. Wall Street Journal. Jan. 2, 2019. https://www.wsj.com/articles/popular-weather-app-collects-too-much-user-data-security-experts-say-11546428914

[61] "While you track Pokémon, Pokémon Go tracks you." Josh Hafner. USA Today. July 11, 2016. https://www.usatoday.com/story/tech/nation-now/2016/07/11/while-you-track-pokmon-pokmon-go-tracks-you/86955092/

[62] "Pokémon Go can see everything in your Google account. Here's how to stop it." Jason Cipriani. CNET.com. July 11, 2016. https://www.cnet.com/how-to/pokemon-go-google-account-access/

spread, game developer Niantic admitted to an error and allowed only "basic" Google profile information to be accessed.

A 2018 feature of Pokémon GO, called Adventure Sync, allows users to track and import their daily steps by linking the game to their phone's health app, either iOS HealthKit or Android Google Fit. Players' steps (and calories burned) are counted throughout the day—even when they're not using the game. Niantic CEO John Hanke wrote in a blog post that Adventure Sync was meant to inspire gamers to get outside and walk, and might lead to notoriously sedentary gamers losing weight.[63] The game's updated privacy policy now notes it "will not use data collected through Apple HealthKit or through Google Fit for marketing or advertising purposes" and that users must opt in to using this feature.

To learn if the social media, game and weather apps on smartphones are collecting location data, users must review the individual app's privacy policy and what, if any, permissions the user has—sometimes unknowingly—provided. While some apps will fess up to sharing location data in real time, others reserve the right to store the data indefinitely and sell it to third parties. Android users can check out AppCensus (https://www.appcensus.mobi) or PrivacyGrade (privacygrade.org) and see what information is being stored and shared by their favorite free apps. See the "Data Control" section of this report for tips on how to control access to user data.

Vehicles

Most of the millions of new cars sold every year are "connected," having built-in navigation systems, diagnostic tools, and the capability of transferring data to and from the vehicle. According to BI Intelligence, approximately 82 percent of all new cars will be "connected" by 2021.[64] Some experts expect that nearly all new cars will be equipped with tracking technology within a few short years.

Add to that the growing number of data-collecting apps and devices used for vehicle-based services. Apps like Google Maps and Spotify are replacing built-in navigation systems and traditional or satellite radio.[65] Connecting a smartphone to a car, via Bluetooth or a USB connection, enables the vehicle to access everything on it, from the contacts list and call log to text messages and location.[66]

Along with apps, insurance industry programs encourage customers to trade their data for discounts, resulting in an environment where nearly every vehicle and driver has the potential to be tracked.

---

[63] "Never miss a step—Introducing Adventure Sync." John Hanke. Niantic. Oct. 25, 2018. https://nianticlabs.com/blog/adventuresync/

[64] "Automotive Industry Trends: IoT Connected Smart Cars & Vehicles. Andrew Meola. Business Insider. Dec. 20, 2016. https://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10

[65] Ibid.

[66] "Tracking Technology: Your Car Is Definitely Watching You—But That Might Not Be a Bad Thing." Kristen Hicks. The Zebra. Feb. 20, 2018. https://www.thezebra.com/insurance-news/5576/tracking-tech-good-and-bad/

Despite the growing quantity of vehicle and driver data, there is relatively little regulation around how it is collected and used, who owns it or how it must be protected. The dearth of regulation leaves consumers' privacy at risk and their rights in question.[67]

Auto manufacturers and dealers

There are no laws that prescribe how all the data captured by your car can be used,[68] or who owns it.[69] Data gathered from event data recorders are the lone exception.

Virtually all new cars in the U.S. since 2014[70] have an integrated "black box," not unlike the flight recorders in commercial airplanes.[71] These event data recorders (EDRs) capture information on more than a dozen variables—such as your speed, braking activity and use of seat belts—in the seconds or minutes just before or during a crash.[72] The devices don't track location and don't transmit the data anywhere.

A vehicle's EDR typically is accessed only if someone needs the data—for an accident investigation, for example. Under the federal Driver Privacy Act of 2015, EDR data is the property of the vehicle owner or lessee, and it can't be accessed by anyone without the owner's permission except under certain circumstances, such as a court order or legal investigation.[73] Seventeen states also have enacted EDR privacy statutes echoing the provisions of the federal law.[74]

Given the paucity of vehicle data protection rules, manufacturers have attempted to reassure consumers that their data is not being misused. In 2014, 20 automakers pledged to meet or exceed commitments contained in the Automotive Consumer Privacy Protection Principles,[75] which purport to: provide customers with clear, meaningful information about the types of information collected and how it is used; provide ways for customers to manage their data; and obtain affirmative consent before using geolocation, biometric or driver behavior information for marketing, and before

---

[67] "Who Owns the Data Your Car Collects?" Jeff Plungis. Consumer Reports. Last updated May 2, 2018. https://www.consumerreports.org/automotive-technology/who-owns-the-data-your-car-collects/

[68] "Data Derived From Connected Cars Raise Concerns." Tom Krisher. Claims Journal. Dec. 27, 2018. https://www.claimsjournal.com/news/national/2018/12/27/288453.htm

[69] "Cars Suck Up Data About You. Where Does It All Go?" John R. Quain. New York Times. July 27, 2017. https://www.nytimes.com/2017/07/27/automobiles/wheels/car-data-tracking.html

[70] "Obama Bypasses Congress to Mandate Black Boxes for All Cars—Beginning in '14." Pete Winn. CNSNews.com. Dec. 13, 2012. https://www.cnsnews.com/news/article/obama-bypasses-congress-mandate-black-boxes-all-cars-beginning-14

[71] Harris Technical Services. Viewed on March 5, 2019. http://harristechnical.com/

[72] "Event Data Recorder." Viewed on March 5, 2019. National Highway Traffic Safety Administration (NHTSA). https://www.nhtsa.gov/research-data/event-data-recorder

[73] H.R. 22—FAST Act. Congress.gov. 2015-2016. https://www.congress.gov/bill/114th-congress/house-bill/22/text#toc-H7E76328B2CD946219201C9FF6470C49

[74] "Privacy of Data from Event Data Recorders: State Statutes." Viewed on March 5, 2019. National Conference of State Legislatures. http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx

[75] Auto Alliance. Viewed on March 5, 2019. https://autoalliance.org/connected-cars/automotive-privacy/participating-members/

sharing such information with unaffiliated third parties for their own use.[76] The Alliance of Automobile Manufacturers committed to reviewing these privacy principles at least every two years to evaluate whether personal information was appropriately protected.

To skirt, yet technically fulfill, the "affirmative consent" portion of the commitment, automakers often write consent into their sale, lease and service contracts[77] or the user agreements required to register or activate vehicle features (like the navigation app).[78] Most automakers will, theoretically, let owners decline having their data collected, but that information typically is buried in the fine print. Unlike denying data collection to a gaming app, it is possible that opting out of having a vehicle collect data could pose risks to driver safety and diminish the car's functionality—for example, the inability to use semi-autonomous driving features.[79]

The move to develop industry privacy principles wasn't entirely altruistic: Being proactive regarding data privacy concerns is one way for the industry to try to muffle cries of "privacy abuse" from consumers and avoid new regulations that could get in the way of future data collection. Consumer advocates are vocal about wanting to see more transparency, more consumer control and greater regulation.[80]

The auto manufacturers' commitment to safeguarding customers' privacy cannot camouflage the industry's interest in eventually monetizing the data; there's great potential for knitting it together for use in targeted marketing, either directly or through third parties. A 2016 report by McKinsey & Company estimated that global revenue from car data monetization could hit $450 to $750 billion by 2030.[81]

For now, though, automakers are wary of alienating customers or violating stricter laws in other countries by massive collection and sharing of owner data.[82] There are signs that such restraint may not last long: Otonomo,[83] an Israeli startup that pitches itself as "a car data marketplace that enables the sharing of vehicle data between auto

---

[76] "Consumer Privacy Protection Principles." Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc. Nov. 12, 2014. https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf

[77] "Tracking Technology: Your Car Is Definitely Watching You—But That Might Not Be a Bad Thing." Kristen Hicks. The Zebra. Feb. 20, 2018. https://www.thezebra.com/insurance-news/5576/tracking-tech-good-and-bad/

[78] "Automakers adopt protocols to handle, protect consumer data in connected car era." Gabe Nelson and Ryan Beene. Automotive News. Nov. 13, 2014. https://www.autonews.com/article/20141113/OEM11/141119926/automakers-adopt-protocols-to-handle-protect-consumer-data-in-connected-car-era

[79] Data Derived From Connected Cars Raise Concerns." Tom Krisher. Claims Journal. Dec. 27, 2018. https://www.claimsjournal.com/news/national/2018/12/27/288453.htm

[80] "Consumer Reports: Is your car collecting data about you?" Michael Finney. ABCNews.com. May 17, 2018. https://abc7news.com/automotive/consumer-reports-is-your-car-collecting-data-about-you/3503827/

[81] "Monetizing Car Data." McKinsey & Company. September 2016. https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx

[82] "Cars Suck Up Data About You. Where Does It All Go?" John R. Quain. New York Times. July 27, 2017. https://www.nytimes.com/2017/07/27/automobiles/wheels/car-data-tracking.html

[83] Otonomo website. Viewed on March 5, 2019. https://otonomo.io/

manufacturers and mobile application developers," sifts through worldwide legal requirements to help companies stay in compliance while using consumer data.

Another way location data can be tracked is if the lender that finances a customer's auto purchase or lease installs a GPS tracker on the vehicle—just in case the consumer stops paying the loan and the dealer needs to repossess the vehicle.[84] The industry argues that use of the technology allows them to sell to those with poor or no credit because it reduces a lender's risk and repossession costs, but privacy advocates and consumer protection agencies are urging safeguards that strengthen disclosure requirements and prevent misuse.[85]

While all these methods of gathering data on drivers are worthy of scrutiny, it's hacking that could ultimately pose the greatest risk to consumer privacy and safety. For example, in 2017, over half a million records belonging to SVR Tracking were discovered publicly accessible online. SVR is a company that specializes in continuous vehicle tracking as a tool for sellers and lenders to recover their financed vehicles. The exposed data file contained information on approximately 540,000 SVR accounts, including email addresses, passwords, and some license plate and vehicle identification numbers (VINs).[86]

Insurance

Many of the biggest U.S. auto insurance companies, including Allstate, State Farm, Progressive and Nationwide, promote programs that monitor customers' driving to customize insurance rates and/or provide discounts (called usage-based insurance, or UBI). The data typically is collected through a plug-in device, though it's also possible to tap the original equipment installed by car manufacturers[87] or gather information via smartphone. At least one company uses the car's built-in OnStar security system to gather data. The information collected includes everything from speed, acceleration and braking force to time of day and location.[88]

For now, at least, participation in any of the "telematics" programs is voluntary, and companies disclose what data they're tracking.[89] However, the absence of wide-

[84] "Used Car Dealers Using GPS Tracking to Monitor Car Financing." LiveViewGPS Inc. Jan. 15, 2015. https://www.liveviewgps.com/blog/car-dealers-gps-tracking-monitor-car-financing/
[85] "Federal Agency Begins Inquiry Into Auto Lenders' Use of GPS Tracking." Michael Corkery and Jessica Silver-Greenberg. New York Times. Feb. 19, 2017. https://www.nytimes.com/2017/02/19/business/dealbook/gps-devices-car-loans.html
[86] "Passwords to Over a Half Million Car Tracking Devices Leaked Online." Dell Cameron. Gizmodo. Sept. 21, 2017. https://gizmodo.com/passwords-to-access-over-a-half-million-car-tracking-de-1818624272
[87] "Usage-based Insurance and Telematics." National Association of Insurance Commissioners. Jan. 17, 2019. https://www.naic.org/cipr_topics/topic_usage_based_insurance.htm
[88] "How connected car tech is eroding personal privacy." Erin Biba. BBC. Aug. 9, 2016. http://www.bbc.com/autos/story/20160809-your-car-is-not-your-friend
[89] "Tracking Technology: Your Car Is Definitely Watching You—But That Might Not Be a Bad Thing." Kristen Hicks. The Zebra. Feb. 20, 2018. https://www.thezebra.com/insurance-news/5576/tracking-tech-good-and-bad/

reaching laws protecting consumer privacy in this area makes it difficult to determine if insurers are using that data in unexpected ways.[90]

A 2018 University of Connecticut report on the topic identifies the lack of clarity around just who owns the telematics data as a "disadvantage" for consumers: "Especially for devices that have been installed by the insurer at no cost to the insured, the insurance companies believe that they own the data, not the policyholder."[91]

The author also calls for regulation: "As the telematics insurance continues to grow in market share, new regulations may be needed in order to ensure the privacy of customer data and their fair treatment. There are currently no standards of data collection in each state; it is up to the insurers to decide what kinds of data they want to collect and how they will collect it. The states should step in and specify what kinds of data could be collected, how detailed these data could be, and how long the storage period should be for these data. Furthermore, the states should clarify who owns the data and ask the insurance companies to specify how they will use the data."[92]

The National Association of Insurance Commissioners (NAIC) acknowledges that usage-based insurance programs raise privacy concerns.[93]

Rental cars

Most rental cars, including those owned by carsharing company Zipcar, are equipped with navigation and GPS technology.[94] While the data collected has previously been used by some rental companies to fine drivers for rental agreement violations such as speeding or crossing a state line, that type of usage is less prevalent now.[95] (In the case of the speeding fines, the court struck down such usage. In other cases, questionable usage has raised the ire of customers and garnered unfavorable publicity.)[96]

---

[90] "How connected car tech is eroding personal privacy." Erin Biba. BBC. Aug. 9, 2016. http://www.bbc.com/autos/story/20160809-your-car-is-not-your-friend

[91] "Evolution of Insurance: A Telematics-Based Personal Auto Insurance Study." Yuanjing Yao. Honors Scholar Theses. 590. May 1, 2018. https://opencommons.uconn.edu/srhonors_theses/590

[92] Ibid. Page 18.

[93] "Usage-based Insurance and Telematics." National Association of Insurance Commissioners. Jan. 17, 2019. https://www.naic.org/cipr_topics/topic_usage_based_insurance.htm

[94] "Can GPS tracking stop customers from stealing rental cars? In California, a new debate over privacy begins." Peter Holley. Washington Post. April 10, 2018. https://www.washingtonpost.com/news/innovations/wp/2018/04/09/can-gps-tracking-stop-customers-from-stealing-rental-cars-in-california-a-new-debate-over-privacy-begins/

[95] "Is Your Rental Car Company Spying on You and Your Driving? Here's How They Do It." Robert McGarvey. TheStreet. March 26, 2015. https://www.thestreet.com/story/13089306/1/is-your-rental-car-company-spying-on-you-and-your-driving-heres-how-they-do-it.html

[96] "Some Rental Cars Are Keeping Tabs on the Drivers." Christopher Elliott. New York Times. Jan. 13, 2004. https://www.nytimes.com/2004/01/13/business/business-travel-some-rental-cars-are-keeping-tabs-on-the-drivers.html

Today, use of location data by the large rental companies is generally limited to scenarios involving a police report, such as vehicle theft.[97] Driver tracking is more likely to be done by small or luxury rental car companies—those for whom a single stolen or abused vehicle could have a significant financial impact.

Generally speaking, it is legal to use a GPS device to monitor a rental car if the vehicle owner authorizes the use of GPS[98] on the car, and if the tracking is disclosed.[99] However, there may be state rules about how and when the data can be accessed. Until recently, California law prohibited rental car companies from locating a missing vehicle using GPS sooner than seven days after it was due to be returned.[100] In 2018, the state reduced the wait time to 72 hours after the car's return due date. Before activating any electronic surveillance on a past-due vehicle in California, the rental company must give the customer 24-hour notice.[101]

Regardless of whether the rental car itself is being tracked, drivers who sync their smartphone with a rental car to use apps and data on a personal device while traveling allow the vehicle and location-enabled apps, such as Google Maps, to collect and store data such as where the car has been, as well as other information (device name, call log, messages, etc.).

While it is technically possible to erase that data, it's not something most renters are aware is a risk. Nor do most consumers realize they can delete what has been captured or know how to do it.[102] (See the "Data Control" section of this report for instructions on how to delete.)

Ridesharing services

The use of GPS is central to ridesharing services such as Uber and Lyft, but for some riders, there is at least some level of consumer control possible.

Uber's privacy policy states that it collects location data on passengers when the Uber app is running in the foreground, and sometimes when it's running in the background, "if

---

[97] "Is Your Rental Car Company Spying on You and Your Driving? Here's How They Do It." Robert McGarvey. TheStreet. March 26, 2015. https://www.thestreet.com/story/13089306/1/is-your-rental-car-company-spying-on-you-and-your-driving-heres-how-they-do-it.html

[98] "Is It Legal to Mount a GPS Device Inside My Car?" Matthew Izzi. LegalMatch. March 5, 2018. https://www.legalmatch.com/law-library/article/gps-tracking-laws.html

[99] "Is Your Rental Car Company Spying on You and Your Driving? Here's How They Do It." Robert McGarvey. TheStreet. March 26, 2015. https://www.thestreet.com/story/13089306/1/is-your-rental-car-company-spying-on-you-and-your-driving-heres-how-they-do-it.html

[100] "Can GPS tracking stop customers from stealing rental cars? In California, a new debate over privacy begins." Peter Holley. Washington Post. April 10, 2018. https://www.washingtonpost.com/news/innovations/wp/2018/04/09/can-gps-tracking-stop-customers-from-stealing-rental-cars-in-california-a-new-debate-over-privacy-begins/

[101] "California Governor Signs Law Reducing Wait Time to Track Stolen Vehicles." Michaela Kwoka-Coleman. Auto Rental News. Sept. 11, 2018. https://www.autorentalnews.com/313063/california-governor-signs-law-allowing-gps-tracking-of-stolen-rental-vehicles

[102] "How to Wipe Your Private Phone Data from a Rental Car." Amanda Woods. Adventures All Around. Nov. 16, 2016. https://adventuresallaround.com/how-to-wipe-your-private-phone-data-from-a-rental-car/

this collection is enabled through your app settings or device permissions." Users who don't want their location data collected in the background should adjust the app and device settings. Uber makes clear that you can still use its ridesharing app with location collection disabled, but you'll need to enter your pickup and drop-off locations manually. Of course, location information will still be collected through the driver's app during your trip and linked to your account

Lyft's privacy policy states: "When you open Lyft on your mobile device, we receive your location. We may also collect the precise location of your device when the app is running in the foreground or background. If you label certain locations, such as "home" and "work," we receive that information, too."[103]

While Lyft's privacy policy claims you can turn off location sharing at any time (through your device), it notes that Lyft will not be able to provide ridesharing services without it.[104]

For rideshare users who have not turned location collection off, tracking typically starts when the ride is requested and ends at drop-off. (Uber did, temporarily, track riders' location for five minutes *after* their rides ended, but they ceased the controversial practice in 2017.)[105] However, Norton, maker of privacy and security software, notes that "if riders don't turn off location access after completing their rides, the app could potentially track and collect data around the clock on where the user is, where they go, and, sometimes, even how long they stay there."[106]

Both Uber and Lyft's privacy policies include standard disclosures and disclaimers about when and with what third parties they might share rider data, but the greatest risk to riders' privacy may come from the companies' own (non-driver) employees. In January 2018, Lyft acknowledged investigating an employee's anonymous allegation that Lyft staff were accessing rider data, including phone numbers and trip history, without a valid business reason, going so far as to track their significant others and well-known public figures.[107] The incident was similar to a 2014 accusation by a journalist that Uber had used an internal company tool (God View) to track her location, without her permission, when she was late for a meeting.[108]

Regardless of where the threat comes from—hackers, the ridesharing company, its employees or some other entity—the takeaway is that consumers' privacy is precarious.

---

[103] "Lyft Terms of Service." Last updated on Feb. 6, 2018. Viewed on March 5, 2019. https://www.lyft.com/terms

[104] Ibid.

[105] "Uber will no longer track your location after your ride is over." Amar Toor. The Verge. Aug. 29, 2017. https://www.theverge.com/2017/8/29/16219542/uber-location-tracking-app-ios-android-privacy

[106] "How ridesharing services can take your privacy for a ride." Symantec. Viewed on March 5, 2019. https://us.norton.com/internetsecurity-privacy-ridesharing-privacy-ride.html

[107] "Lyft investigates privacy abuse claim." Dave Lee. BBC. Jan. 26, 2018. https://www.bbc.com/news/technology-42827636

[108] "Uber allegedly tracked journalist with internal tool called 'God View.'" Rich McCormick. The Verge. Nov. 19, 2014. https://www.theverge.com/2014/11/19/7245447/uber-allegedly-tracked-journalist-with-internal-tool-called-god-view

Lyft's privacy policy might sum it up best: "Even though we take reasonable precautions to protect your data, no security measures can be 100% secure, and we cannot guarantee the security of your data."[109]

Connected cars and other "smart" technologies have made data collection ubiquitous in the "Internet of Things" era. While vehicle data collection offers some valuable benefits, a lack of wide-reaching regulation regarding collection, ownership and storage/security leaves consumers and their data open to risks.

Food delivery apps

The popularity of food delivery apps is no surprise. Yet, food delivery apps couldn't do what they do without location tracking. Whether accessed through a user's cell phone, computer or tablet, the food delivery services connect users to local eateries and bring restaurant meals to our doorsteps. Food delivery apps also rely on ridesharing companies, whose drivers deliver the food.

UberEats, Caviar, DoorDash and Seamless

Consumer Action analyzed four of the most popular food delivery apps—UberEats, Caviar, DoorDash and Seamless—all of which require access to the geolocation of customers' phones in order to carry out the delivery service.

We found many downsides for consumers when food delivery companies collect location data without restraint. They include invasive marketing, such as unwanted promotions from local restaurants; unwitting public exposure of their restaurant reviews, driver ratings and other feedback; data breaches; and misuse of data by third parties. Worse yet is the very real prospect of insurance companies using food delivery data to gauge a consumer's health "risk level" and raise their rates for eating fast food or ordering too frequently from that Italian restaurant with the health code violations down the street.[110] Conclusions could also be unfairly reached about the sedentary nature of people who aren't willing to walk out to collect their own food.

Once users give permission to access their location data, the apps collect the longitude and latitude of the phone using GPS, the unique IP address of the device in use, and public Wi-Fi information. Once a user opens an app and orders food, the app constantly pings the phone's location to provide updates on how long it will take for the driver to arrive, and it tracks the driver en route.

The data these apps collect comes largely from the user, who agrees to provide location information in exchange for the convenience of receiving delivery service. This agreement is disclosed in the apps' privacy policies and terms of service, which, of

[109] Lyft Terms of Service." Last updated on Feb. 6, 2018. Viewed on March 5, 2019. https://www.lyft.com/terms

[110] "Why the Life-Insurance Industry Wants to Creep on Your Instagram." Nathan Heller. New Yorker. Feb. 26, 2019. https://www.newyorker.com/culture/cultural-comment/why-the-life-insurance-industry-wants-to-creep-on-your-instagram

course, most users don't read. Location data also can come directly from the food couriers. UberEats' privacy policy states "location information will be collected from the driver during your trip and linked to your account, even if you have not enabled Uber to collect your location information."

While location data is mainly used for facilitating pickup and delivery of food orders, most apps can also use it to compile users' order history and, consequently, track their movement throughout time. In the case of food delivery apps, this includes from where and at what time you order—whether it's from home on Friday nights, from school on Tuesdays, *or* from church during a recurring AA meeting. The *New York Times* explained how easy it is to identify people's lifestyles and behaviors, and even their identities, based on the data these types of apps collect.[111] Even though consumers' names might not be tied to an app, their unique identifying IP addresses are. Many consumers don't realize that the apps they download are tracking them through their phone.

Comparable privacy policies

Each of the food delivery app privacy policies Consumer Action reviewed stated that the information associated with a customer's device could include the device's unique identifier and mobile network information. UberEats tells customers: "We may collect information about the devices you use to access our services, including the hardware models, device IP address, operating systems and versions, software, file names and versions, preferred languages, unique device identifiers, advertising identifiers, serial numbers, device motion information, and mobile network information."

Food delivery apps also use customer information to personalize content and advertising. For example, apps send alerts about new restaurants that have opened in the user's area. In addition, they can use personal information for resolving disputes. For example, the consumer may claim a delivery driver took longer to arrive than the driver claims, and location data helps the company verify the facts and take action.

Consumers also may inadvertently reveal information about their location from the public reviews they leave online through the food delivery apps. A user might write, for example, "As a hungry diner in Brooklyn who loves Grimaldi's Pizzeria on Front St…" Sometimes reviews include real names and photos, often pulled from Facebook if the user logged in with their Facebook credentials or synced the app to their Facebook account when they installed the food delivery app on their mobile device. Syncing the app to social media may also allow users' delivery status (e.g., "I just ordered pizza from Grimaldi's through [insert app name]") to be posted automatically to the social media network unless the user explicitly forbids this. UberEats enables "features to personalize your Uber account, such as creating bookmarks for your favorite places, and to enable quick access to previous destinations."

[111] "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller and Aaron Krolik. New York Times. Dec. 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

The privacy policies of the four popular food apps made clear that they collect and retain information about when and where food delivery orders and transactions occur, along with the name of the transacting party, the address of the person ordering, a description of the transaction, the products bought through the service, and payment information, including the type of payment and the amount.

Seamless states: "We use your information to fulfill your [delivery] requests…and to customize content on our sites (e.g., the restaurants that will deliver to your location)." Uber discloses that it reserves the right to use the information it collects for "testing, research, analysis and product development."

While some apps may not explicitly state how long they retain customer data, DoorDash is not unique in holding on to it for quite some time, perhaps indefinitely. The company states in its privacy policy: "We are required to retain records relating to previous purchases through our Services for financial reporting and compliance reasons. In addition, because of the way we maintain certain services, after you delete certain information, we may temporarily retain backup copies of such information before it is permanently deleted." Seamless states that its "third party service providers will retain Personal Information for at least the period reasonably necessary to fulfill the purposes outlined in this privacy policy, unless a longer retention period is required or permitted by law."[112]

Sharing data with third parties

The food delivery apps stated in their privacy policies that they reserve the right to share users' personal data with third parties. This data includes the user's name, phone number, address, the restaurants a user orders from, ratings the user leaves on the app (of drivers and restaurants), and other information the user provides directly or, as DoorDash calls it, "information collected automatically." When location and other data are shared for advertising purposes it's often with social media companies like Facebook or Google that facilitate targeted local ads. The apps also share personal data with the restaurants they partner with. These restaurants, in turn, can share the data with additional third parties.

Food delivery apps also share data with third parties for payment processing. For instance, Caviar shares user data with its payment processing parent company, Square, Inc., and may provide it to law enforcement for the prevention of fraud and for what UberEats deems "unsafe activities." And Seamless states that it reserves the right to share users' personal info with third parties that provide services on its behalf, such as "payment processing, website hosting, data analysis, infrastructure provisioning, IT services, customer service, email delivery services, targeted advertising and marketing, and other similar services." Finally, Seamless added that it would share personal info as it "believes appropriate" under applicable laws, including "laws outside of your country of residence."

[112] "Grubhub Privacy Policy." Viewed on March 1, 2019. https://www.grubhub.com/legal/privacy-policy

Two of the four companies we analyzed also share user information with third-party corporate partners. Caviar shares user data with its parent company, Square, Inc., and Seamless shares with partner companies Grubhub, Eat24 and MenuPages.com. Seamless states: "Grubhub is the party responsible for the management of jointly-used personal information."

Each of the four apps discloses that third parties are able to use cookies and other technologies to track user behavior, and specifically user IP addresses—which allows for location tracking.[113]

It's no surprise that all of the apps were careful to eschew any blame or liability for any misuse of data due to third parties' privacy policies. DoorDash says "such [third party] websites [that it chooses to share data with] are not under our control and we are not responsible for their privacy policies or practices."

Buried in the privacy policies of all of the apps were caveats that they could sell or give away personal user information, "in connection with (including, without limitation, during the negotiation or due diligence process of) a corporate merger, consolidation, or restructuring; the sale of substantially all of our stock and/or assets; financing, acquisition, divestiture, dissolution of all or a portion of our business, or other corporate change." DoorDash words its policy similarly, stating that: "In the event of sale, transfer, merger, reorganization, dissolution, or similar event we may transfer your information to one or more third parties as part of that transaction."

From these disclosures, it's obvious that once a user's data has been shared with a food delivery app, it's "out of the box," and there's really no way to stuff it back in. And there's also no good way to track how the companies are using your data after the initial transaction. At the end of each of the privacy policies, the food delivery apps state that it is the consumer's responsibility to check back in (on their privacy policy webpages) to discover any changes to the app's policies. Only one app—DoorDash—stated that it would email consumers about privacy policy updates.

Wearable technology

Wearable technology (or "wearables") has exploded in recent years, and is only expected to grow in popularity as a way to manage one's health and wellbeing. Two of the most popular devices, watches and wristbands, act as health monitors that track personal fitness metrics such as the user's sleep patterns, heart rate and how many steps are taken daily. Depending on the device, it also can track the user's exact location and daily routes via GPS, Bluetooth, IP Address, crowd-sourced Wi-Fi hotspot and cell tower location tracking. These wearables can sync to your mobile phone and various installed apps. This information is usually uploaded to the device's cloud software, where users can access the information and track their progress, typically through a related app.

[113] "How to track your lost smartphone with an IP address?" IP Location. Nov. 18, 2018. https://www.iplocation.net/track-lost-smartphone-with-ip-address

Tracking data and keeping oneself accountable for daily steps, exercise and rest can change behavior and lead to longer, healthier lives. Insurance company John Hancock now requires customers in its Vitality program[114] to use activity trackers if they want to be eligible for discounted life insurance premiums and other perks. Customers can withhold fitness data, but that results in higher premiums, which could put life insurance policies out of reach for some.

So who owns the personal data that's collected through wearables, and what happens when the data is accessed by third parties that don't have users' express permission? If a wearables company or fitness app goes out of business, might it sell customers' data to advertisers or other companies? Consumer Action examined the privacy policies of the makers of the top five wearables—Apple Watch, Xiaomi, Huawei, Fitbit and Samsung—to learn what data they collect and share with third parties.

Detailed health data

All these wearables companies collect daily sleep, activity and heart rate information. Every company except for Samsung mentioned collecting very precise data coordinates of its users, utilizing a combination of GPS, Bluetooth, IP address, crowd-sourced Wi-Fi hotspots, third-party apps and cell tower locations.

With the exception of Samsung, the companies noted sharing de-identified data with third parties, and every company stated that they share personally identifiable information with "partners" and affiliated companies. Only two companies stated what they would do with users' personal data if the company went out of business: Huawei said it reserves the right to sell users' information, and Fitbit stated that it would be committed to protecting the confidentiality of users' data in such a case.

Even though these wearables claim to share only anonymous user data, having more than one location data point, like the location of one's home and work, means that it would take only a brief Google search to potentially identify the name of a user. Once there are three, four or five data points linked to a location, the chances of pinpointing the user increases dramatically. Identifying someone becomes easier if the device transfers information about where the user stays every night, works every day, and where their heart rate goes up in response to exercise—for example, their gyms or exercise classes.

The Center for Digital Democracy warns in a privacy report on wearables that data from many of these devices already is being integrated into a "digital health and marketing

[114] "John Hancock Leaves Traditional Life Insurance Model Behind to Incentivize Longer, Healthier Lives." Ana Senior. John Hancock. Sept. 19, 2018. https://www.johnhancock.com/content/johnhancock/news/insurance/2018/09/john-hancock-leaves-traditional-life-insurance-model-behind-to-incentivize-longer--healthier-lives.html

ecosystem, which is focused on gathering and monetizing personal and health data in order to influence consumer behavior."[115]

This ecosystem includes hospitals, pharmaceutical and insurance companies, drug stores, health departments and research organizations. The report warns of profiling racial and ethnic backgrounds and medical conditions that might be used to discriminate against people when the data was collected, sold or even hacked. For example, if a wearables company suffered a massive data breach and life or health insurance companies gained access to previously protected data, users might see increases in the cost of annual premiums, or insurance policies might be cancelled all together.

Users of wearables might assume that their personal health stats are protected under the Health Insurance Portability and Accountability Act (HIPAA), but this federal law only applies to official medical records handled by "covered entities," including medical facilities, insurance companies and pharmacies. Neither the Food and Drug Administration (FDA), the Federal Trade Commission, nor the Federal Communications Commission have express regulatory jurisdiction over these devices,[116] leaving consumers more vulnerable should their data get hacked.

Fitness apps

Along with wearable devices, fitness apps allow users to monitor exercise and daily calorie intake. Many of these apps sync with wearables and encourage users to share their daily workouts and meals with the app's "community" (app users). What users might not realize is how widely this information can travel and how it can reveal previously unconsidered information. The fitness app Strava made the news last year when it pinpointed users at U.S. military bases in countries like Afghanistan, Iraq and Syria.

Strava says it's designed for those who are serious about fitness, including many service members, who track their running and biking routes and share them with the Strava community. The company published a global "heat map" that showed the workout routes of users who posted publicly. In this map, two of the largest coalition bases in Afghanistan could easily be inferred. What was more concerning: The commonly used routes that connect bases revealed that American military members traveled those routes by car, foot or bicycle. This information could have left troops vulnerable to attack while off base.

---

[115] "Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection." Kathryn C. Montgomery, Jeff Chester and Katharina Kopp. Center for Digital Democracy. Aug. 29, 2017. Page 14. https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf

[116] Ibid. Page 16.

The Strava heat map wasn't just a privacy nightmare for the U.S. military. It appears that Strava users in Taiwan exposed the location of one of Taiwan's "secret" missile command centers.[117]

While Strava users willingly share a fair amount of personal data, a bigger security concern might be what information hackers glean about members of our military from "private" data. Security analysts warned that even though the heat map doesn't specifically name people, users could be identified by cross-referencing app user data with social media and online searches.[118]

Researchers have shown repeatedly that anonymized data is fairly easy to crack if two or more data points are available. Privacy researcher Yves-Alexandre de Montjoye showed how the majority of the population with mobile phones could be personally identified from their phone's anonymized location data.[119] He and his team analyzed the mobile location data of 1.5 million people over 15 months—with no other personally identifying information—and were able to identify 95 percent of the people using just four data points about place and time. Fifty percent of users could be identified from just two data points.

In response to the heat map scandal, Strava now allows users to create Privacy Zones that restrict sharing any activities within that zone. However, Strava still collects that data.[120]

While fitness apps and wearables might help you achieve a healthier lifestyle, a fair amount of skepticism is warranted as to the personal data collected and how it's being shared. As wearable technology advances, and devices begin to monitor even more biometric markers, like EKGs, oxygen intake and blood pressure rates, there is increasing optimism that these devices will improve chronic conditions and healthcare services. However, this information is exceedingly valuable to a wide range of companies, making people extremely vulnerable, especially since major data breaches are inevitable. Until solid consumer protections are enacted, users of wearable technology need to take care to understand what companies are doing with our most sensitive data.

---

[117] "Fitness-Tracker App Exposes Security Flaws at Taiwan's Missile Command Center." Jeffrey Lewis. Daily Beast. Jan. 28, 2018. https://www.thedailybeast.com/strava-fitness-tracker-app-exposes-taiwans-missile-command-center

[118] "Strava Fitness Spp Can Reveal Military Sites, Analysts Say." Richard Pérez-Peña and Matthew Rosenberg. New York Times. Jan. 29, 2018. https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html

[119] "Unique in the Crowd: The privacy bounds of human mobility." Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel. Scientific Reports. March 25, 2013. https://www.nature.com/articles/srep01376

[120] "Strava Privacy Policy." Viewed on March 1, 2019. https://www.strava.com/legal/privacy

Employee tracking

With employees working remotely, traveling on business, and operating independently in the field, companies say they have more reason than ever to monitor workers' location. Employees do not always agree.

Service companies managing landscapers, office cleaners, work crews, sales teams and delivery drivers often track employees' location. Firms that sell location data tracking services—via an app or through GPS—maintain that the data helps employers make real-time decisions to improve productivity. Staff can log in and out of locations, and managers can dispatch crews, schedule visits, navigate and adjust routes, receive accurate mileage counts, and locate field staff. Location data might help companies protect overseas staff coping with political unrest or another crisis situation far from home.

The travel and expense management company SAP Concur offers the Concur Locate service, which employs artificial intelligence to monitor employee location globally. Concur's website states: "In an emergency, Concur Locate can pinpoint employees' locations, help you communicate with them, and even send help if necessary."[121] It also tracks credit card expense data and Uber ridesharing data to ensure employee safety. Concur says it does not track employees' movements for any other purposes.

Another firm, International SOS, offers TravelTracker to help companies locate overseas employees during a crisis. It provides companies with travelers' flight, hotel and car rental details and their contact information. In the case of a crisis, TravelTracker sends automatic alerts to managers on how many employees are in a given country, and provides travel and incident advice. Overseas staffers also can receive health and security/safety alerts.

Companies that sell location tracking tools to businesses say their apps allow employers to monitor time spent in transit versus time spent doing the job. The employee can start and stop the tracking clock, or the tool can be set to automatically track when an employee enters and leaves a site. Using "geofencing" (monitoring mobile devices in a particular area), employee monitoring firm Hubstaff offers companies an app to track employees' GPS location. The data is stored for 30 days.

Apps like myGeoTracking also use geofencing (which can monitor an area using GPS, Wi-Fi or RFID technology) for determining employees' arrival and departure times and compiling "location breadcrumb reports" that explain "where your employees have been."[122]

[121] "Concur Locate homepage." Viewed on March 1, 2019. https://www.concur.com/en-us/concur-locate
[122] "Real-time Employee Location Tracking App." MyGeoTracking. Viewed on March 1, 2019. https://www.mygeotracking.com/solutions/employee-gps-tracking-increase-visibility-accountability

Deloitte, a Big Four accounting firm, offers a real-time location tracking app as part of its suite of services to clients who need to track out-of-state or overseas business travel and employment for tax and auditing purposes.[123]

The data collected by Deloitte's app includes employees' nationalities, home locations, passports and business travel. The employee enters travel dates, locations and reasons for travel to help businesses book and approve work travel.[124] In Europe, employees' personal information is protected under strong European Union data protection rules, but those rules do not necessarily apply to workers from other countries.

Big accounting firm Ernst & Young offers clients a smartphone app called Tracer, which uses GPS and enables employees to transmit their location twice a day for tax, immigration and compliance purposes. Ernst & Young says that no personal information about employees is transmitted.

Accounting firm PricewaterhouseCoopers offers MyMobility, an employee app, and TravelWatch for tracking employees' travel history.

As far back as 2012, the technology research firm Aberdeen Group found that 62 percent of companies with so-called "field employees" were using GPS to track staff.[125]

When tracking becomes a problem

Location information gathered during employees' off hours can reveal quite personal information. Tracking isn't always turned off on company vehicles and phones after hours. Off-the-clock tracking could disclose health information, doctor's visits, sexual orientation, religious or other group affiliations that damage relationships between employees and employer and hurt employee morale. Employers that track employees while on their own time could end up in court.[126]

The app TSheets reports employee location to supervisors every five to 10 minutes, but the app shuts down when an employee clocks out. However, a TSheets survey said that about one-third of employees surveyed said their employers track them; one in 10 said they were tracked with GPS 24 hours a day. One in five (of the 1,000 survey respondents) said the tracking was switched on without warning.[127]

---

[123] "Managing business travelers." Deloitte. Viewed on March 1, 2019. https://www2.deloitte.com/us/en/pages/tax/articles/managing-business-travelers-tax-global-employer-services.html

[124] "Diary of a (compliant) time traveller: The mobile revolution in business travel." Deloitte. 2018. https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/tax/deloitte-uk-diary-of-a-compliant-time-traveller.pdf

[125] "Some companies are tracking workers with smartphone apps. What could possibly go wrong? Andrea Peterson. Washington Post. May 14, 2015. https://www.washingtonpost.com/news/the-switch/wp/2015/05/14/some-companies-are-tracking-workers-with-smartphone-apps-what-could-possibly-go-wrong/

[126] "Monitoring Employees' Off-Duty Conduct." Nolo. Viewed on March 1, 2019. https://www.nolo.com/legal-encyclopedia/monitoring-employees-off-duty-conduct-29994.html

[127] "Survey: The Surprising Truth: What Employees Think of GPS Tracking in the Workplace." TSheets by QuickBooks. November 2016. https://www.tsheets.com/gps-survey

At some companies, employees can manually shut off location tracking, but in one case, a California woman sued her employer for firing her for disabling GPS tracking on her company phone during her off hours.[128] Her location was monitored during her non-working hours. The employee may have relied on California invasion of privacy law, since most state laws do not address employee tracking on a mobile device. This case, Arias v. Intermex Wire Transfer, settled out of court, and the outcome remains private.[129]

Privacy protection

The U.S. Constitution protects us from unreasonable searches and seizures—from *government* actions. Typically the government, including the police, needs a warrant to monitor individuals; the Fourth Amendment may not protect workers if their employer chooses to track them.

There is no federal law to prevent GPS tracking by employers. Some state laws—California, Texas, Virginia, Minnesota and Tennessee—require a vehicle owner's consent before tracking, but if a company owns the vehicle that an employee drives, then consent is automatic. The state of California prevents tracking "to determine the location or movement of a person," except in company-owned vehicles.[130] Employees can assert a right to privacy, but their rights are very unclear. Whether the employee was ever notified of (and consented to) being tracked, and who owns the mobile device or vehicle, will factor into future court privacy violation decisions.

Even without well-defined legal protections, many companies and attorneys recommend[131] a set of employer best practices for employee location tracking:

- Notify employees in advance;
- Limit information gathering to legitimate business need;
- Only track during working hours;
- Explain how the data will be used and secured; and
- Obtain written acknowledgement of the policy from employees.[132]

---

[128] "Worker fired for disabling GPS app that tracked her 24 hours a day." David Kravets. Ars Technica. May 11, 2015. https://arstechnica.com/tech-policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day/

[129] "GPS Tracking of Employee Devices: How Much Is Too Much?" Kamika S. Shaw. On Labor. May 8, 2017. https://onlabor.org/gps-tracking-of-employee-devices-how-much-is-too-much/

[130] "GPS Tracking Laws in California." LiveViewGPS Inc. Viewed on March 1, 2019. https://www.liveviewgps.com/blog/gps-tracking-laws-california/

[131] "There's An App For That: Considerations in Employee GPS Monitoring." Jennifer M. Holly. Seyfarth Shaw. Jan. 26, 2017. https://www.calpeculiarities.com/2017/01/26/theres-an-app-for-that-considerations-in-employee-gps-monitoring/

[132] "Monitoring your employees through GPS: What is legal, and what are the best practices?" Elizabeth Austermuehle. Impact (Greensfelder, Hemker & Gale, P.C.). Feb. 18, 2016. https://www.greensfelder.com/business-risk-management-blog/monitoring-your-employees-through-gps-what-is-legal-and-what-are-best-practices

Companies like Deloitte counsel clients to notify employees that they are being tracked, inform them why monitoring is needed, and commit—in writing—to not track employees during non-working hours. Deloitte recommends that companies give workers as much control as possible over tracking, agree to use the data solely for business purposes, and retain data only if legitimately necessary.

Some companies—with employee buy-in—have gone as far as to implant microchips in employees.[133] A Wisconsin company offered to implant RFID chips (the size of a grain of rice) into employees' hands. About 40 staffers[134] took part in the voluntary program[135] in 2017. The chip is similar to what's implanted in pets to find them if they're lost. In April 2017, it was reported that a Swedish company was planning to do the same to 150 of its employees to monitor how long they work, and to allow employees to log on to computers, pay for lunch at the company cafeteria and open doors with the swipe of a hand.[136]

"In the past, surveillance was seen as something bad. It intruded on our lives. We were often willing to put up with it because it provided benefits, such as security. But that didn't mean we liked it. Now it seems we no longer see surveillance as an intrusion on our privacy," noted organizational behavior professor André Spicer of City University in London. "Today, many employees think the latest forms of digital surveillance are 'cool'. At the Wisconsin vending machine company, they volunteered to be chipped. So did the entrepreneurs based in the Stockholm tech hub."[137]

Yet not all observers agree. According to Michel Anteby, a Boston University associate professor of sociology and business who has studied how monitoring affects employees at the TSA and other workplaces, "the more employees are watched, the harder they try to avoid being watched, and the harder management tries to watch them."[138]

[133] "Why Bosses Can Track Their Employees 24/7." Kaveh Waddell. The Atlantic. Jan. 6, 2017. https://www.theatlantic.com/technology/archive/2017/01/employer-gps-tracking/512294/
[134] "Surveillance used to be a bad thing. Now, we happily let our employers spy on us." André Spicer. Aug. 4, 2017. The Guardian. https://www.theguardian.com/commentisfree/2017/aug/04/surveillance-employers-spy-implanted-chipped
[135] "Three Square Market Microchips Employees Company-Wide." Three Square Market press release. PRLog. July 20, 2017. https://www.prlog.org/12653576-three-square-market-microchips-employees-company-wide.html
[136] "Bosses are already tracking employees with microchip implants." New York Post. April 3, 2017. https://nypost.com/2017/04/03/bosses-are-already-tracking-employees-with-microchip-implants/
[137] "Surveillance used to be a bad thing. Now, we happily let our employers spy on us." André Spicer. Aug. 4, 2017. The Guardian. https://www.theguardian.com/commentisfree/2017/aug/04/surveillance-employers-spy-implanted-chipped
[138] "The Employer-Surveillance State." Ellen Ruppel Shell. The Atlantic. Oct. 15, 2018. https://www.theatlantic.com/business/archive/2018/10/employee-surveillance/568159/

Data Control: Consumers' limited control over location data collection

Users have limited control over others accessing a lot of their location data—in fact, probably far less than they imagine. How much control users have over the collection, use and sharing of their location data depends on a variety of factors, including who is doing the collecting, what, if any, regulations govern the collector, and whether the user has given permission (intentionally or unknowingly) to collect and use the data.

Even when users have some control, they may not know how to implement it. In this section, we explain the control users do have to better protect themselves, broken down by the industries we've examined in this paper.

For Consumer Action's recommendations on how to address data protection and consumer privacy, turn to page 46 of this report.

Internet service providers (ISPs)

When users connect to the internet via a phone carrier's network, each user's private internet protocol (IP) address is constantly and automatically connecting them to the nearest cell phone tower, which is one way users' location can be identified. When signing a cell phone or internet service contract, users often inadvertently "opt in" to allowing ISPs to collect and distribute sensitive personal data, including location. This consent typically is buried in the fine print.[139]

Unlike for Google or Facebook, there are no settings to turn off to halt location tracking by an ISP, although, as explained (under "Social media") above, users can turn off location tracking (GPS) preferences within their cell phones. Even so, cell phone towers and routers are still being "pinged" with each user's unique identifying (IP) address[140] and its location, which is sent to the ISPs.[141]

In other words, simply adjusting privacy settings on a mobile device can give consumers a false sense of control. Customers probably wouldn't glean this from any of the major ISPs' complex privacy policies. Take Verizon's policy, for instance, which explains that when users turn off location settings, "the device stops collecting your location and stops transmitting location information to apps on the device, including Verizon apps." What Verizon fails to mention[142] is that while the device is not sending location information to *apps,* Verizon—as an ISP—maintains the ability to obtain, collect and

[139] "Why Is Your Location Data No Longer Private?" Krebs on Security. May 26, 2018. https://krebsonsecurity.com/2018/05/why-is-your-location-data-no-longer-private/
[140] "The Inside Secrets About IP Addresses and Geolocation." WhatIsMyIPAddress.com. Viewed on March 1, 2019. https://whatismyipaddress.com/geolocation-accuracy
[141] "How Do Police Track Cell Phones?" Keith Evans. Techwalla. Viewed on March 1, 2019. https://www.techwalla.com/articles/how-do-police-track-cell-phones
[142] Verizon Privacy Policy. Viewed on March 1, 2019. https://www.verizon.com/about/privacy/full-privacy-policy

distribute users' location information[143] (which the company states in its terms of service, and which is evidenced by cases in which police or emergency response teams ask for access to the data and ISPs deliver it). Verizon still has access to customer data via cell phone towers and metadata.[144] To stop location data collection by any mobile broadband provider, users must turn off their phones.

Telecoms vs. ISPs

Verizon, AT&T, Comcast and Charter/Spectrum are telecom carriers *and* ISPs. Carriers only can release customer information to third parties after obtaining opt-in consent. While the law applies to all *carriers,* it does not apply to ISPs. Currently, there are no specific federal customer data protection laws that apply to ISPs.

While dual telecom/ISP companies may state that they allow users to opt out of having Customer Proprietary Network Information shared with third parties, this CPNI "opt out" only applies insofar as the company is operating as a telecom. CPNI is "information that relates to the quantity, technical configuration, type, destination*, location,* and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[145]

For instance, under the section "Information we share," Verizon states that it releases CPNI to its "family of companies" (third parties, marketers), but that customers can limit this kind of sharing of CPNI by calling 800-333-9956. What Verizon is *not* saying is that a customer's CPNI is only protected as it applies to its role as a telecom company. Again, it does not apply to its ability to access and share customer data as an ISP. ISPs know where you go on the internet, but they can't see what you do once you're on secure websites. However, knowing that you are visiting Cancer.com gives them information from which they could draw inferences.

A 2017 FCC data privacy rule would have limited the personal data that ISPs could collect[146], but it was revoked in 2018.[147] It would have prevented ISPs from selling or sharing location and other personal data without explicit opt-in consent from users.[148]

---

[143] "How Do Police Track Cell Phones?" Keith Evans. Techwalla. Viewed on March 1, 2019. https://www.techwalla.com/articles/how-do-police-track-cell-phones

[144] "How the Supreme Court's Ruling on Cell Phone Metadata Changes Privacy Rights." Ben Goggin. Inverse. June 22, 2018. https://www.inverse.com/article/46308-the-supreme-court-just-ruled-to-protect-cell-phone-location-data

[145] "47 U.S. Code § 222. Privacy of customer information." Cornell Law School Legal Information Institute. https://www.law.cornell.edu/uscode/text/47/222

[146] "FCC Adopts Broadband Consumer Privacy Rules." Federal Communications Commission. Oct. 27, 2016. https://www.fcc.gov/document/fcc-adopts-broadband-consumer-privacy-rules

[147] "House Votes To Allow Internet Service Providers To Sell, Share Your Personal Information." Consumerist. Consumer Reports. May 4, 2018. https://www.consumerreports.org/consumerist/house-votes-to-allow-internet-service-providers-to-sell-share-your-personal-information/

[148] "What does the new ISP data-sharing rollback actually change?" Russell Brandom and Jacob Kastrenakes. The Verge. March 31, 2017. https://www.theverge.com/2017/3/31/15138526/isp-privacy-bill-vote-trump-marsha-blackburn-internet-browsing-history

Consumer Action recommends that users read their ISP's privacy policy to try to glean what, if any, data sharing practices they can limit. Any disclosures and choices likely pertain to CPNI *telecom* data—not to data use by the company in its role as an ISP.

This telecom-ISP distinction is one of the loopholes that could be closed if Congress adopted meaningful federal data protection regulation (see the "Data protection recommendations" section for more information).

Social media

Limit sharing

Users should familiarize themselves with the privacy settings in their social media accounts. All social media platforms enable users to control who sees what they share. Users typically can set the default to sharing with their "friends" list, or customized smaller lists, rather than making what they share public. Users also can limit the amount of personal information they reveal in their account profile, such as the city they reside in or the company they work for, which can provide location information to an unintended audience. It's usually possible to prevent one's social media content from being indexed by search engines. Whenever possible, disable automatic location tags in posts and photos.

Facebook

In addition to not oversharing, Facebook users can protect their location data by limiting tracking within the Facebook app (see "App-level permissions," below) and choosing not to click the "Check In" pin (which announces real-time location) when posting.

Users also can turn Facebook's "Location History" feature on or off, and delete the history for a particular day or entirely. "Location History" is a timeline of specific places you have been, organized by day. The history reflects the location information received from your device through "Location Services."

Facebook has updated its "Access Your Information" tool, which calculates users' primary location at the city or ZIP code level. Now, very small ZIP codes or cities are combined so that users' primary location is less precise.

For Android phones, the company recently introduced a new control called "Background Location," which allows users to not share their location with Facebook when they aren't using the app.[149] This addresses Android's all-or-nothing location access options.[150]

Facebook says it does not share location data with others unless a user chooses to, such as by turning on their "Nearby Friends" tool.

---

[149] "Improving Location Settings on Android." Facebook Newsroom. Feb. 20, 2019. https://newsroom.fb.com/news/2019/02/location-settings-android/

[150] "Facebook now lets you block background location tracking on Android." Jacob Kastrenakes. The Verge. Feb. 20, 2019. https://www.theverge.com/2019/2/20/18233424/facebook-android-location-data-privacy-controls

Snapchat

To prevent others from accessing location data, Snapchat users can set their profile to ”Ghost Mode” in “Settings.” By enabling Ghost Mode, user location on the Snap Map is hidden from anyone else. (Users will still be able to access the Snap Map and see the location of their Snapchat friends if the friends have Ghost Mode turned off.)

Google

After logging in to a Google account, users can check the location markers Google has gathered on their My Activity page (https://myactivity.google.com/). Users also can review all the apps they've given access to in their Google account.

To stop location tracking, users have to turn off “Web & App Activity” *and* “Location History.” Doing so will stop exact location markers from being collected and linked to their Google profile.

Google warns that when “Location Services” is off:

- Your device's location isn't shared with any apps, and features that use location may not work properly.
- Google “Location Services” won't collect data to improve location-based services.
- You can get search results and ads based on your IP address.
- You can't see where your device is if you lose it.
- You can't share your device's location with anyone via Google Maps, but you can still send it to first responders in an emergency.[151]

To further limit what Google knows about them, users can choose to activate the “Private browsing” mode in Google Chrome, or use a different browser entirely (DuckDuckGo and Brave are two privacy-oriented options). Signing out of your Google account rather than staying permanently logged in will also increase privacy.

App-level permissions

During download, apps usually request access to the user's location, camera, contacts, etc. While some apps legitimately require location information to function properly, apps that demand location data but don't need it to function as intended should be scrutinized before download, given the unwarranted privacy trade-off.

iOS (Apple) devices allow users to choose if and when a particular app has access to location information: never, always, or only when the app is in use. This typically is done in a tab under “Settings” named “Location Services” or something similar, under which all the apps are listed. Until now, Android offered only an all-or-nothing approach to app location permissions: either deny the app any access to your location or grant it full use

[151] “Manage your Location History.” Google Help Center. Viewed March 1, 2019. https://support.google.com/accounts/answer/3118687?hl=en

of your location.[152] Android Q, a software update still in beta in May 2019, will give Android users the same flexibility that iPhone users have to allow location access sometimes, always or never.[153]

Apps that don't need location information, like most games, can be set to "Never." Other apps should only track location when in use; there's no reason for most apps to track users all the time.

Turn location tracking off by device

Smartphones give users a fair amount of control over location tracking, offering the option to turn off location tracking entirely—and it's a fairly simple process (typically done in "Settings," under the "Privacy," "Location" or similar tab). Users even can delete their location history—data collected when tracking *wasn't* turned off—though the process is a bit more complicated on the Android (Google) than on an Apple iPhone.

Vehicles

"Connected" cars

Most automakers disclose in the owner's manual or in a sales or service agreement that tracking is going on.[154] Most carmakers will let owners opt out of having their data collected, but notice of that right typically is buried in the fine print. Plus, opting out could pose risks to users' safety and cause a number of inconveniences, from not knowing when the car needs service to not being able to use the embedded navigation system.[155]

GPS on subprime borrowers

Lenders that extend credit to car buyers with subprime or no credit history reserve the right make the financing contingent on having GPS installed on the vehicle, to be able to track it down and, in case of default on the loan, repossess it. Technically, car buyers are free to refuse the tracking, but the lender will almost certainly refuse to finance the sale. Once car buyers agree to be tracked, disabling the GPS device becomes a violation of the loan contract.

---

[152] "Facebook now lets you block background location tracking on Android." Jacob Kastrenakes. The Verge. Feb. 20, 2019. https://www.theverge.com/2019/2/20/18233424/facebook-android-location-data-privacy-controls

[153] "Android Q: Everything you need to know!" Joe Maring. Android Central. April 10, 2019. https://www.androidcentral.com/android-q

[154] "Automakers adopt protocols to handle, protect consumer data in connected car era." Gabe Nelson and Ryan Beene. Automotive News. Nov. 13, 2014. https://www.autonews.com/article/20141113/OEM11/141119926/automakers-adopt-protocols-to-handle-protect-consumer-data-in-connected-car-era

[155] "Data Derived From Connected Cars Raise Concerns." Tom Krisher. Claims Journal. Dec. 27, 2018. https://www.claimsjournal.com/news/national/2018/12/27/288453.htm

Auto insurance

Usage-based unsurance programs, which use telematics (transmission-enabled software or devices) to gather driver and vehicle data, are voluntary and optional. If the insurer provided and/or installed the telematics device, it could be argued that the insurer owns the data. Since these programs are voluntary, users have the option to not participate and not be tracked. Companies generally disclose what data they are tracking, but that might not be required unless your state has such a regulation.

Rental cars

Generally, it is legal to use a GPS device to monitor a rental car if the vehicle owner (the rental car company) authorizes the use of GPS[156] on the car, and if the tracking is disclosed.[157] Beyond that, state law may govern when the data can be accessed.[158] In California, rental car companies are prohibited from locating a missing rental car using GPS until 72 hours past the car's due date. Before activating the GPS, the rental company must give the customer 24-hour notice.

Users can limit tracking in a rental car by not syncing their smartphone with the vehicle. This also avoids potential access to users' data by future rental car customers, or by buyers of the data if a rental car company sells it. For users who do sync their smartphone, they can greatly reduce the privacy risks by deleting the data from the car's "infotainment" system before returning the vehicle. Go to the "Settings" menu, locate your device in the list of previously paired Bluetooth gadgets, and delete it.[159]

Ridesharing

When using a ridesharing platform, there's nothing users can do to prevent having their location tracked through the driver's app.

Uber allows users to use its ridesharing app with location collection disabled on their phones, but they'll need to enter their pickup and drop-off locations manually.[160] It also offers some app settings to allow users to fine-tune their preferences if they don't want to turn location services off completely.[161]

---

[156] "Is It Legal to Mount a GPS Device Inside My Car?" Matthew Izzi. LegalMatch. March 5, 2018. https://www.legalmatch.com/law-library/article/gps-tracking-laws.html

[157] "Is Your Rental Car Company Spying on You and Your Driving? Here's How They Do It." Robert McGarvey. TheStreet. March 26, 2015. https://www.thestreet.com/story/13089306/1/is-your-rental-car-company-spying-on-you-and-your-driving-heres-how-they-do-it.html

[158] "California Governor Signs Law Reducing Wait Time to Track Stolen Vehicles." Michaela Kwoka-Coleman. Auto Rental News. Sept. 11, 2018. https://www.autorentalnews.com/313063/california-governor-signs-law-allowing-gps-tracking-of-stolen-rental-vehicles

[159] "How to Wipe Your Private Phone Data from a Rental Car." Amanda Woods. Adventures All Around. Nov. 16, 2016. https://adventuresallaround.com/how-to-wipe-your-private-phone-data-from-a-rental-car/

[160] "Uber Privacy Policy." Last modified on May 25, 2018. Viewed on March 5, 2018. https://privacy.uber.com/policy/

[161] "How Uber uses rider location information (iOS)." Uber Help. Viewed on March 5, 2019. https://help.uber.com/riders/article/how-uber-uses-rider-location-information-ios?nodeId=741744cb-125c-4efc-ab3f-4a977940ac87

Food delivery apps

To minimize food delivery app location privacy concerns, customers do *not* have to allow these companies to automatically access their location data. Instead, users can manually enter the delivery address in the app.

Be aware that driver location will always be tracked and linked to your (the service user's) account when you use a delivery service app, even if you have not enabled the service to collect your own location information.

To further limit automatic location data collection, users should not sync the delivery app to their Facebook or Twitter accounts. Instead, they should use an email address to log in.

For users who *are* allowing food delivery apps to access their location through their cell phone when they place an order, set the apps to not run in the background, and close the apps when not in use. This will prevent them from accessing your device's GPS when not needed for service.

Wearable technology

Fitness trackers can tell where you are at any given moment, down to a few yards. In most cases, users can stop wearable devices from collecting and potentially sharing their exact location data points (and biometrics) with others.

Check app privacy settings

Most wearables require users to download a corresponding app to transfer data from the wearable device to the interactive app on the phone. Typically an account is connected to the user's phone number or email address. Be sure to use an inconspicuous account name and strong password when setting up the account—preferably not one you have used before.

Go into the app's settings and privacy controls to review the data you are sharing and with whom. This is where users can change the privacy settings. If there is a social media element linked to the app, users should check to see if they have been automatically placed into a public profile that might share the user's wearable metrics without the user realizing; consider setting the account to private. Also check the wearable's website, which might have privacy settings that users can't control from the phone or device.

Turn off phone geo-tracking

Android and iPhone users have the option of denying access to location information. See the "Turn location tracking off by device" section, above, for information.

Review privacy policies

This advice applies to all industries: Check out what the company says it will do with users' information and what rights users have to control it. We found the privacy policies for the top five wearables by searching online. Location data can be collected from GPS, Bluetooth, IP address, crowd-sourced Wi-Fi hotspots and cell tower locations, plus other sources that share users' locations.

Employee tracking

There is not much that employees can do to limit tracking (other than quit) if the employer's policy applies to all employees and is a requirement of the job. Employers may contract with outside firms for employee tracking. Some employee tracking firms disclose their level of data sharing in their privacy policies. Some say they share personal employee data with the employer and other persons that the "Company [employer] chooses to provide access" to.[162]

Employees at firms that use tracking should take care to learn about the technologies used by their employer and to read the company's employee location tracking policy, if any. They might also want to search for information on any state laws that might exist related to employee tracking. A few states prohibit employers from requiring employees to wear (or implant) RFID or microchip tracking devices.[163]

Laws in some states—California, Texas, Virginia, Minnesota and Tennessee—require a vehicle owner's consent before tracking, but employers aren't required to obtain employee consent if the worker is driving a company-owned vehicle. While employees that drive company-owned vehicles home may not be able to limit tracking in the vehicle even when off the clock, those with employer-provided mobile phones may want to turn the devices off when they are not working. For employees who use a personal vehicle for work, the employer cannot install a tracking device in the car without the owner's permission. However, employers may easily coerce employees' permission if the employees believe that refusing would cost them the job. Employees who feel their employers are acting unfairly or illegally should consider bringing legal action.

Data protection recommendations

With hidden profiles being assembled about each one of us, precision tools that can track us just about anywhere, and a growing data store to help others judge us, there's plenty for consumers to mistrust, and even fear. Every day we make conscious or unconscious trade-offs with our data for the sake of convenience or to gain access to free online content.

---

[162] "Concur Technologies, Inc. Processor Privacy Statement." Viewed on March 1, 2019. https://www.concur.com/en-us/processor-privacy-statement

[163] "Company Offers Employees Implanted Microchips." Cynthia Blevins Doll. Cross Border Employer. Aug. 21, 2017. https://www.lexology.com/library/detail.aspx?g=21f67626-aca1-4bf8-a239-acecf824636f

It's clear that consumers have far too little control over the data that defines our lives, affects our opportunities for jobs, loans, housing and insurance, and reveals our location—even our identity—often without our knowledge or consent.

When location data is collected and shared, we are exposed to a myriad of real and potential harms. Too often, consumers are cavalier about their privacy. But, as ACLU attorney Matt Cagle noted to the *New York Times*: "Privacy is really about being able to define for ourselves who we are for the world and on our own terms. That's not a choice that belongs to an algorithm or data broker, and definitely not to Facebook,"[164] or any of the other technology giants and purveyors of personal data, either.

Privacy specialist and former FTC chief technologist Ashkan Soltani said, **"**Most consumers simply didn't have the time or experience to navigate the personal-data economy on their own,"[165] which is why consumers need a set of comprehensive data protection laws.

In 2012, the Obama administration unveiled a consumer privacy bill of rights that called for limits on what data companies could collect and gave consumers more control over how their data was used. But this did not materialize because, as with any discussion of limiting online privacy invasions and uses of personal data, the devil is in the details. Everyone agrees in principle about the need for strong laws to protect individuals' privacy and security online. But many attempts to write and pass comprehensive federal privacy regulation have failed on the details.

Still, we need to pass a robust federal data protection law that would require those seeking data about an individual to obtain express consent prior to collecting, using or sharing a user's personal data.

Federal data protection legislation must give individuals basic protections, including the right to:

- Know what personal data is collected, used, stored, shared and sold about each of us, and for what purpose;
- Access and obtain a copy of that data;
- Correct inaccurate data;
- Delete data;
- Prevent the sharing or sale of personal data to third parties; and
- Sue a company that violates these protections.

The companies that collect, share and sell our data must be held to the highest standards of privacy and security.

---

[164] "Privacy Is Too Big to Understand." Charlie Warzel. New York Times. April 16, 2019. https://www.nytimes.com/2019/04/16/opinion/privacy-technology.html

[165] "The Unlikely Activists Who Took On Silicon Valley—and Won." Nicholas Confessore. New York Times. Aug. 14, 2018. https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html

We have models, such as the European Union's (EU) General Data Protection Regulation (GDPR) (https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en) and California's Consumer Privacy Act (https://www.caprivacy.org/), on which to build a stronger federal law with additional protections. Nimble state legislatures must have the ability to enact stronger state data protection laws to safeguard their citizens.

In 2018, Consumer Action, along with its allies, urged companies like Facebook, Google and Amazon to use the EU's privacy principles and technical compatibility standards as a baseline standard for users worldwide.

GDPR established clear limits for companies, including social media platforms, around the collection of user data, and spelled out the rights individuals have to control that data—including deletion. Social media users must know exactly what is being collected about them, how it is used (for services, marketing and political targeting, for example), whom it is shared with and for what purposes.

Consumer Action has agreed to principles outlining a foundation for a new approach to privacy protection. They call for strong baseline federal legislation; the enforcement of fair information practices (FIPs), such as transparency about business practices, data collection and use limitations; data minimization and deletion; purpose specification; access and correction rights; accountability; data accuracy; and strong confidentiality/security.[166]

On April 12, 2019, Senator Ed Markey (D-MA), a member of the Senate Commerce, Science and Transportation Committee, introduced federal privacy legislation to protect American consumers' personal information. Sen. Markey's bill would prohibit companies from using individuals' personal information in discriminatory ways; require companies to protect and secure the personal information that they hold; establish a centralized FTC website that tells consumers about their privacy rights and requires companies to use easy-to-read short-form notices provided directly to consumers; ensure companies collect only the information they need from consumers in order to provide the requested services; and enable state attorneys general to protect the interests of their residents and bring action against companies that violate the privacy rights of individuals. The legislation includes a private right of action empowering individuals to defend their privacy rights.[167]

Sen. Markey also teamed up with Sen. Josh Hawley (R-Mo.) to introduce legislation to update the U.S. Children's Online Privacy Protection Act (COPPA) by prohibiting internet companies from collecting personal and location information from anyone under 13 without parental consent, and from anyone 13-15 without the user's consent. The legislation also creates an "eraser button" so that parents and kids can delete personal

[166] "The Time Is Now: A framework for comprehensive privacy protection and digital rights in the United States." https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf
[167] "Senator Markey Introduces Comprehensive Privacy Legislation." Office of Sen. Ed Markey. April 12, 2019 https://www.markey.senate.gov/news/press-releases/senator-markey-introduces-comprehensive-privacy-legislation

information, and a "Digital Marketing Bill of Rights for Minors" that limits the collection of personal information. The bill would establish a Youth Privacy and Marketing Division at the Federal Trade Commission, responsible for addressing the privacy of children and minors and regulating marketing directed at them.[168]

Data protection agency

Consumer Action supports the establishment of a federal data protection agency to create and enforce privacy protection rules and oversee companies that desire to use individual data for company gain.

Internet service providers (ISPs)

Mobile phones are the No. 1 personal tracking device, since most owners carry them everywhere. Consumer Action has called on policy shapers and lawmakers to ensure that ISPs, in particular, be required to obtain express consumer consent before sharing or selling any personal or sensitive customer data—including location, health, financial and other private information.

In April 2017, President Trump nullified[169] a groundbreaking privacy rule passed by the Federal Communications Commission that would have regulated ISPs' use of Customer Proprietary Network Information under the Telecom Act. ISPs would have been prohibited from collecting, storing, sharing and selling certain types of customer information—including customer location details—without individuals' explicit consent.[170] Consumer Action supported the rule, and believes that ISPs and telecoms must be required to obtain explicit consent to share user data, including geolocation information. Existing FCC rules should be enforced to keep data brokers from buying and exploiting customer location data from telecoms/ISPs.

Last summer, the Supreme Court, in U.S. v. Carpenter, ruled that cell phone location information searches by the government fall under the Fourth Amendment and that access by law enforcement requires a warrant. Meaningful federal or state penalties should be applied if law enforcement accesses real-time location information from cell phones without a warrant.

Apps

There are no U.S. laws that specifically provide privacy rights for consumers using apps (smartphone software). These programs can and do collect a lot of data from

---

[168] "Lawmakers introduce bill to protect children's data privacy." Emily Birnbaum. The Hill. March 12, 2019. https://thehill.com/policy/technology/433608-lawmakers-introduce-bill-to-protect-childrens-data-privacy

[169] "Trump has signed repeal of the FCC privacy rules. Here's what happens next." Brian Fung. Washington Post. April 4, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/

[170] "Republicans voted to roll back landmark FCC privacy rules. Here's what you need to know." Brian Fung. Washington Post. March 28, 2017. https://www.washingtonpost.com/news/the-switch/wp/2017/03/28/republicans-are-poised-to-roll-back-landmark-fcc-privacy-rules-heres-what-you-need-to-know/

consumers, who generally give consent when downloading and using the app. The Federal Trade Commission *can* limit clearly unfair and deceptive practices and require that apps stick to what they promise in their privacy policies.

Consumer Action doesn't believe that consumers have meaningful control of their personal data if the terms of service require them to waive their privacy rights, and calls for clear prohibitions on the collection of information by apps that is not needed to provide the service the app was designed for. Any sharing or sale of personal data—including biometric and location data—collected by apps should be prohibited without express, written permission from the app user.

Wearable technology

Wearable devices that track biometric and location information collect health and wellness data but, in most cases, are not regulated as medical devices or as "covered entities" under health privacy laws. Since no U.S. regulatory agency has clear jurisdiction over data collected through wearable devices, the Federal Trade Commission Act could be expanded to include wearables data. This would give the FTC explicit authority to enforce consumers' privacy rights and determine if companies are misleading consumers by failing to maintain security for sensitive information.

Consumer Action believes that all data collected through wearable devices should be considered sensitive health information at the federal level, and laws must be written to make this a clear distinction. (Such data may fall under state health privacy laws, which often are more comprehensive than their federal counterparts.)

Autos

Automakers should provide customers with clear, user-friendly disclosures about the types of information collected by their cars, how it could be used, and what controls consumers do and don't have over the data. The use or sharing of geolocation, driver behavior and other data for marketing purposes should require affirmative consent ("opt in"), separate from the purchase or lease agreement, service registration or owner's manual.

Rental car companies should be required to include with the rental agreement, and inside the vehicle, a data collection notice that explains what happens when a smartphone is synced with a car, and should provide easy-to-follow instructions, specific to that model of car, for how to delete the device and collected data at the end of the rental period.

Federal laws and regulations must hold these companies responsible for protecting the consumer data they collect, including guidelines for holding on to data (the shorter the term, the better) and require that consumers receive notice of breaches.

Food delivery apps

Food delivery apps must be subject to regulations governing how they share the data they collect, and be prohibited from sharing it with any entity that is not engaged in providing the service. All food apps should follow Uber's lead and allow consumers to permanently delete their data using privacy settings offered *within the app itself*. All apps should provide customers with the ability to turn off data collection and location tracking when the app is not in use.

Another way

While Consumer Action doesn't believe that self-regulatory schemes work to protect consumer privacy, we have seen some innovative examples of profitable companies committed to protecting consumer data. For example, the privacy-focused search engine DuckDuckGo has created a model that operates profitably without relying on storing, sharing or selling consumer data. DuckDuckGo earns commissions when consumers purchase from Amazon and eBay—*without* sharing customers' personal information.

The company says the money they make from data tracking is based on keyword searches. A consumer types dishwasher and, soon after, sees dishwasher ads. This approach does not require search history information, nor is it tied to individuals. DuckDuckGo has said that Google, Facebook and other big tech companies would still be "wildly profitable" if they stopped behind-the-scenes tracking and storing of data because they would still have the enormous audience reach advertisers pay for.

But we can't rely on the good will of select firms to protect our personal information. We need strong federal data protection laws to *compel* companies to protect our sensitive information, safety and right to control what is collected about us. We need to give states the flexibility to exceed federal laws if they need to, and give individuals a right to hold companies accountable in court when they break the law.

That is why, as an organization, Consumer Action holds passage of strong baseline federal privacy law as today's chief goal in consumer protection. The Digital Age demands it, and we have, as a nation, tarried too long in achieving it.

Conclusion

In survey upon survey, consumers voice their concern about responsible use of their data and protection of their privacy, while also revealing their dependence on the very technology that "spies" on them. Though persistent pressure on the companies that, virtually unchecked, gather, use and share detailed data on Americans has resulted in some increased privacy options, the real control over consumers' location data remains firmly in the hands of the data collectors.

Consumers won't turn their backs on technology, and technological advancements that enable the collection of even more data (self-driving cars, for example) won't stall. Since industry can't be relied upon to adequately self-govern and put consumers' privacy interests ahead of their own business interests, the onus is on the U.S. government to adopt strong laws that protect and empower Americans.

Addendum: Location data should be used only with permission, finds survey

Smartphones, apps, websites and automotive devices can gather and use information based on the current location of your device in order to provide a variety of location-based services. But beyond their obvious utility, should companies retain and use data about where you've been for other purposes? The answer was a fairly resounding no.

The insights come from a survey conducted by Consumer Action to gauge consumer opinion about location data collection and sharing. Answers were provided by 2,475 people, who responded to our emails, website posts and social media messaging. Respondents came from all states. Those who answered an optional question about age skewed over 40, with a full 61 percent of those who answered saying they were over 60.

In answer to a question about when it's okay for companies to collect personal location data, the majority of respondents (66.5%) chose "Only as needed to provide a location-dependent service (such as ridesharing services, maps/directions, roadside assistance, etc.)."

Just over 17 percent chose "Only to provide a location-dependent service OR if I'm getting a benefit or discount" (for example, a retailer coupon or a lower auto insurance rate).

In an open-ended response field, many of the almost 11 percent who wrote something said that it was never okay to collect location data, and some even took us to task for not making this one of the available responses. A few of the open-ended responses made the point that location tracking was a great tool for law enforcement to use when sussing out criminal activity, but it shouldn't be used to track law-abiding citizens.

Fewer than 1 percent chose the response "Anytime—companies have a right to collect information about the customers that use their services."

"I don't understand why corporations and/or their autonomous location computers insist on tracking Americans 24/7. It's actually a Big Brother thing, and if we ever have a tyrannical government, tracking could be a sci-fi nightmare," wrote one respondent. Another commented: "If I want someone to know where I am, I'll phone them myself and tell them. Anything else is invasion of privacy."

We asked if it was ever okay for companies that collect location data to provide a service (rideshare, driving directions, etc.) to keep that data after the service is complete. "No, never" was the response chosen by 56.9 percent, while 31 percent agreed it was okay "only if I previously was asked for, and gave, explicit consent (opted in)."

As to selling or sharing location data with third parties, 83 percent firmly answered "No, never." Just about 15 percent allowed that, "Yes, consumers should assume that the

service providers they use have the right to share, sell and use the location data they collect from their customers/users."

The top concerns regarding the collection and use of location data cited by respondents were: 1) General loss of privacy/lack of control over my personal information (61%); 2) Potential breach (my data could fall into a hacker's or thief's hands) (58%); and 3) Use by companies for profiling (for example, basing insurance premiums on ZIP code) (48%). Other responses—"Use by the government or law enforcement without cause" and "Personal safety risk (could be used by a stalker, my ex-partner, etc.)"—each garnered 43 percent. A little over 40 percent said, "I care equally about all of these."

One respondent noted: "Collection of data should be hacker-proof" (don't we wish!). Another rightfully commented, "Data collection can be used to 'profile' individuals and may lead to harmful discrimination upon the individual." "My data should be owned by me," said another.

Some respondents expressed skepticism about whether it is even possible to control all the data collected about us. "Is it even possible to keep all this info contained, safe, and private? Is it possible to hold any company accountable for the breach of information anymore? I think we're fighting a losing battle with that one." Another wrote: "As a society, we need to better understand how data collection, storage and immediate/long-term use of data we never before had access to is impacting us. It's a dialogue we are not having, and need to."

When asked "Would you stop using a service and/or delete an app if it didn't allow you to turn off or opt out of location data collection?," 69 percent of respondents said they would, while only 22 respondents (0.89%) said they would not. About 15 percent chose "Yes, but only if it were a service or app that has no need to know my location (such as a crossword puzzle or recipe app)." Another 15 percent chose "It would depend on how much I wanted/needed the app."

More than three-quarters of respondents (76.73%) said they had turned off location services on one or more of their smartphone apps, while 13 percent said they didn't know how to turn off location on their internet-enabled devices. As to the actual apps for which people said they most frequently (and knowingly) allowed their location to be tracked, maps and GPS took the lead, with 73 percent of responses, while ridesharing (such as Uber or Lyft) garnered a tad over 20 percent. The other choices (public transportation, retailers/shopping, task apps, social media, food delivery and fitness) got 17 percent or fewer responses. About 11 percent said they didn't use apps.

Respondents were asked about their preferences for how companies they do business with provide notice and disclosures about location data practices. Top responses, chosen by at least 70 percent of respondents, were: "Get my explicit opt-in before collecting my location data, even to provide a service that requires it"; "Prompt me to allow or forbid location data collection each time I access an app"; and "Allow me to have my location data history deleted upon request."

Among the open-ended responses to this question, a number of consumers touched on the lack of transparency in corporate disclosures. One person wrote: “I think all such items should be brief, clear & easy to find, not hidden inside dozens of pages of legalese.” Another noted: “There should be a standard consent form. Consumers aren't well equipped to deal with complicated industry forms. Let Europe lead. The cookie policy led by the EU [European Union] is simple and seems to work well.”

“Asking every single time seems like a pain, but often, even if they publish their policy, it's in fine print...literally and figuratively,” wrote another. “Even if you do read it, months down the road you probably won't even remember giving them the ok. Simpler wording and...perhaps every six months you use the service, a window could pop up reminding you of the policy. More companies need to strive to be transparent, seriously.”

Looking at the survey responses, it appears that many of us have a great awareness of the issues surrounding data collection and privacy. Many place blame squarely on companies that put profits before the rights of individual customers.

As one respondent put it: “The rights of the individual must always be given priority over the rights of businesses or entities. I feel like the speed at which technology has changed has allowed tech companies to exploit the ignorance and naïveté of Americans and global consumers in a way that has defrauded many of us of our right to privacy and liberty without our knowing or being aware of it. These companies cannot be allowed to claim ignorance in this regard.”

The survey ran from Feb. 8 to March 4, 2019, via SurveyMonkey, a web-based surveying tool. Survey results can be found here: https://www.consumer-action.org/downloads/Location-tracking-survey-2019.pdf. Consumer Action prohibits the use of our surveys for commercial purposes.