SJC-12952

IN THE COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

COMMONWEALTH OF MASSACHUSETTS,

v.

JOSIAH ZACHERY

On appeal from a judgment of the Suffolk County Superior Court

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF DEFENDANT-APPELLANT

CAITRIONA FITZGERALD, BBO #673324
Counsel of Record
ALAN BUTLER
MEGAN IORIO
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
fitzgerald@epic.org

Counsel for Amicus Curiae *EPIC*

October 16, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

CORPORATE DISCLOSURE STATEMENT

Pursuant to Supreme Judicial Court Rule 1:21, *amicus curiae* Electronic Privacy Information Center ("EPIC") states that it is a District of Columbia corporation with no parent corporation or publicly held company with a 10 percent

or greater ownership interest. EPIC is a non-profit, non-partisan corporation, organized under section 501(c)(3) of the Internal Revenue Code.

PREPARATION OF AMICUS BRIEF DECLARATION

Pursuant to Appellate Rule 17(c)(5), *amicus* declares that:

(a) No party or party's counsel authored this brief in whole or in part;

(b) No party or party's counsel contributed money to fund preparing or submitting the brief;

(c) No person or entity other than the *amicus curiae* contributed money that was intended to fund preparing or submitting a brief; and

(d) Counsel has not represented any party in this case or in proceedings involving similar issues, or any party in a case or legal transaction at issue in the present appeal.

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy issues.[1]

EPIC routinely participates as *amicus curiae* in cases concerning the impact of emerging technologies and data collection practices on constitutional rights and civil liberties. In particular, EPIC has argued that a warrant should be required under the Fourth Amendment and its state constitutional equivalents for government access to personal data, even if that data is held by a third party. *See, e.g.,* Brief for EPIC et al. as *Amici Curiae* Supporting Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402) (arguing that technological changes since the era of analog phones justify departing from the third-party doctrine); Brief for EPIC et al. as *Amici Curiae* Supporting Petitioner, *Riley v. California*, 573 U.S. 373 (2014) (No. 13-132) (arguing that, because modern cell phone technology provides access to an extraordinary amount of personal data, a warrantless search of a person's cell phone is a substantial and unnecessary infringement of privacy); Brief for EPIC et al. as *Amici Curiae* Supporting Respondent, *United States v. Jones*, 565 U.S. 400 (No. 10-1259) (arguing that

[1] EPIC Appellate Advocacy Fellow Melodi Dincer and EPIC Domestic Surveillance Fellow Jacob Wiener contributed to this brief.

warrantless GPS surveillance by law enforcement enables mass surveillance of the public while operating vehicles on public roads); Brief for EPIC as *Amici Curiae* Supporting Appellant, *Anibowei v. Wolf*, (5th Cir. 2020) (No. 20-1005) (arguing against warrantless searches of the contents of a person's cellphone by law enforcement at the U.S. border).

EPIC has also filed *amicus* briefs before the Supreme Judicial Court on important privacy issues including improper warrantless searches. *See, e.g.*, Brief for EPIC as *Amicus Curiae* Supporting Appellant, *Commonwealth v. White*, 475 Mass. 583 (2016) (arguing that police must obtain a warrant before a school may turn over a student's cell phone); Brief for EPIC as *Amicus Curiae* Supporting Appellant, *Commonwealth v. Connolly*, 454 Mass. 808 (2009) (warning the court of the dangers of warrantless surveillance from GPS tracking systems).

SUMMARY OF THE ARGUMENT

This case concerns the warrantless collection of personal data held by the Massachusetts Bay Transportation Authority ("MBTA"), but its implications stretch far beyond that. The Court's decision in this case ultimately turns on whether and how broadly it adopts the third-party doctrine. EPIC respectfully argues that this Court should reject the third-party doctrine and prohibit the warrantless collection of personal data held by the MBTA and other entities given that individuals must necessarily disclose their personal information to this and other third parties in order to participate in modern society.

Since the Court's 2014 decision to protect cell phone location records in *Commonwealth v. Augustine*, it has become even more difficult for individuals to use services that are essential in the Commonwealth without disclosing their personal data. Companies have ramped up collection of personal information through kiosks and terminals, websites, smartphone apps, wearable devices, and internet-enabled home goods. Consumers today are largely unaware of the volume and sensitivity of data collected about them. Few, if any, would expect the information from the casual tap of a Charlie Card would end up in the hands of law enforcement. And even when individuals knowingly disclose personal information to the businesses or providers with which they transact, they expect their data to be used only for the limited purposes associated with that service. This expectation

aligns with basic principles of data privacy. Data privacy law recognizes that, when an individual provides personal information to a third party for a limited purpose, the individual consents to the use of the personal information for only that limited purpose. Individuals do not expect, and do not consent to, third parties using or disclosing their data for other purposes—and that includes law enforcement.

The third-party doctrine is inconsistent with this fundamental principle of data privacy law, and the warrantless collection of personal data from third parties violates the reasonable expectation of privacy. This case provides the Court with an excellent opportunity to reject the third-party doctrine and to incorporate fundamental privacy principles into the reasonable expectation of privacy analysis. By rooting a decision in the actual expectations of individuals and the underlying privacy law principles, the Court can ensure that privacy is protected even as many aspects of daily life become inextricably linked with digital services. If the Court fails to reject the third-party doctrine now, the right to privacy will rapidly disappear as data-driven technologies and services proliferate. The third-party doctrine is an ancient relic of a bygone era. The time has come to lay it to rest.

ARGUMENT

I. This Court has already recognized that the third-party doctrine is ill suited to the modern world.

In *Commonwealth v. Augustine*, 467 Mass. 230 (2014), this court took an important step toward rejecting the third-party doctrine for one of the most sensitive types of electronic information: location data. The Court recognized that cell site location information ("CSLI") is not "knowingly provided to the telephone company" and that "[n]o cellular telephone user . . . voluntarily conveys CSLI to his or her cellular service provider." *Id.* at 250. This preceded the U.S. Supreme Court's decision on similar lines in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and the Supreme Court's decision there similarly focused on the absence of the consumer's "voluntary exposure" of his data. *Id.* at 2220. The Court also reasoned in *Augustine* that the law should not allow warrantless collection of a "very detailed and extensive information about the individual's 'comings and goings' in both public and private places." *Augustine*, 467 Mass. at 251. The collection of Charlie Card data from MBTA in this case implicates similar privacy interests.[2] A rider who taps their card to get on the T does not know that they are

[2] Each Charlie Card contains a serial number. These numbers are associated with a cardholder when they register their card with the MBTA. Each time a card is used to access public transit, the MBTA collects point-of-entry data. Appellant received a student pass card through the M-7 program, which requires schools to register the serial number of each card provided to students with the MBTA. At the police

creating a time-stamped record of their location that will later be disclosed by MBTA to law enforcement without a warrant. Like GPS and cell phone location records, these Charlie Card logs can be used to track an individual's movements over time. And a rider does not voluntarily disclose this location data because card swipes are necessary for most riders who use the MBTA.

This Court could decide the third-party doctrine question in this case based on its reasoning in *Augustine*. But the Court should take this opportunity to clearly reject the third-party doctrine as applied to modern data collection. There is a fundamental flaw in the third-party doctrine, a flaw that this Court recognized may require complete reconsideration of the doctrine: the misconception that disclosing personal data in order to obtain a service means that the individual assumes the risk that the company or service provider can and will do whatever it wants with that data. That is not a fair or reasonable assumption under modern privacy law and practice; individuals demand and are entitled to much greater care and limitation in the handling of their personal information.

The third-party doctrine was created at a time when data protection law in its modern form did not exist, and data collection practices were limited based on the available technologies and current business practices. The information at issue in

officer's request, the MBTA used Appellant's card's serial number to trace his movements on public transit with MBTA data. This data also allowed officers to access video recordings of the stations Appellant had visited.

Smith v. Maryland, 442 U.S. 735 (1979), for example, was extremely limited—consisting only of basic dialing and routing information for landline telephone calls.[3] But even when *Smith* was decided in 1979, the Supreme Court was sharply divided over the conclusion that this information could be obtained without a warrant. Justices Brennan, Marshall, and Stewart dissented. Justice Marshall in his dissent channeled the nascent principles of data privacy law when he wrote that "[t]hose who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes." *Id.* at 749 (Marshall, J., dissenting).

Three decades later, Justice Sotomayor echoed Justice Marshall, rejecting the assumption that "all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *United States v. Jones*, 545 U.S. 400, 418 (Sotomayor, J., concurring) (2011). Justice Sotomayor's solo concurrence in *Jones* bridged the gap between the Court's majority opinion, which reasoned that the warrantless attachment and use of a GPS tracker to monitor a car over the course of a month

[3] The "pen register" device at issue in *Smith* was "a mechanical device attached to a given telephone line and usually installed at a central telephone facility. It record[ed] on a paper tape all numbers dialed from that line. It [did] not identify the telephone numbers from which incoming calls originated, nor [did] it reveal whether any call, either incoming or outgoing, was completed." *United States v. Giordano*, 416 U.S. 505, 549 n.1 (1974) (Powell, J., concurring in part).

was a *trespassory* search that violated the Fourth Amendment, and the concurring opinions of the remaining Justices who reasoned that tracking an individual's location over time violated their reasonable expectation of privacy. Justice Sotomayor explained that the third-party doctrine's approach was "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.* at 417.

But even after *Jones*, many courts were hesitant to adopt the approach outlined by the five Justices in concurrence. This Court did echo reasoning in *Augustine*, declaring that "the rapid expansion in the quantity of third-party data generated through new technologies raises important questions about the continued viability of the third-party doctrine in the digital age." 467 Mass. 230, 252 n.35 (2014). The Court quoted Justice Sotomayor, declaring that, soon, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id*. (quoting *Jones*, 545 U.S. 400, 417 (Sotomayor, J., concurring)). But the Court stopped short of rejecting the third-party doctrine altogether, and instead made a narrower holding based on the privacy interests at stake in cell phone location data.

In the years since this Court ruled in *Augustine*, the collection and use of personal data has increased exponentially and the need for greater privacy protection has become clear. The time has come to set aside the third-party

doctrine and adopt a more protective warrant requirement to restrict the collection personal data. Companies, schools, transit agencies, and other entities now routinely collect and store vast amounts of personal data during the course of providing essential services and routine interactions with individuals. It is simply not possible to live life without being subject to data collection, and no one should be forced to do so to protect their privacy. Everyday objects like watches, beds, and appliances generate data that was previously unknowable and is now being collected and stored by companies. This information is typically disclosed by the individual for the purpose of obtaining a service. Other information might be incidentally collected by the company while providing the service. But no matter how the data is obtained, individuals expect the data is only to be used for the specified purposes, and not made available to any person or government official on a whim. This fundamental principle of data privacy law respects and enables the individual's right to control how their data is used and whether it is disclosed after it is collected by a company. And data collectors have the obligation to comply with these limitations and refrain from more expansive uses or disclosures absent express consent. The constitutional right to privacy should apply these modern principles—otherwise our civil rights will be quickly eroded by the ongoing evolutions of technology and business practices.

II. The data collected by companies and service providers today is quantitatively and qualitatively different than the information at issue in *Smith* and *Miller*.

Courts are only now coming to grips with how technological and societal changes have altered the most basic premises about what is reasonable and expected when it comes to the collection, use, and disclosure of personal information. More data is created and collected during routine activities today than the Supreme Court could have conceived of in the 1970s. And recent Supreme Court decisions have made clear that this technological and societal shift weighs in favor of stronger constitutional privacy protections. Specifically, the vast quantities of personal data generated by cell phones and other computing devices combined with the uniquely sensitive quality of data that can now reveal every facet of an individual's life require a rethinking of traditional exceptions to the warrant requirement (like the search-incident-to-arrest exception and the third-party doctrine). Furthermore, the widespread adoption of fundamental privacy principles should inform the scope of the constitutional right.

A. The amount of personal data collected and generated through everyday activities is staggering.

The advent and broad adoption of smartphones and other computing devices has made many tasks quicker and easier but has also led to the creation and proliferation of personal data in every facet of life. The common phrase, "There's an app for that," is an officially trademarked slogan that has become the ultimate

siren call of our times. *See* Doug Gross, *Apple Trademarks 'There's an App for That,'* CNN (Oct. 12, 2010).[4] Apps are used to access financial accounts, entertainment, educational content, and even public facilities and benefits. Public transit authorities are not immune from this trend—the MBTA already offers a variety of apps to riders including an app that replaces tickets on the commuter rail. *MBTA-Endorsed* Apps (2020).[5] But while these apps and other digital tools can increase the ease of access to MBTA and other services, there is a growing recognition that such broad data collection poses substantial risk to individuals if there are not adequate legal protections.

One area where data collection has expanded is through smartphone apps. These apps collect data from users directly and in some cases enable third parties to collect data even without their users' knowledge. These apps not only create vast quantities of data, but they also collect sensitive data that never would have existed in the analog world. For example, health monitoring apps offer "access to a category of information otherwise unknowable." *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018). The universe of health and wellness includes apps for sleep tracking, sunlight exposure for vitamin-D monitoring, diet-tracking, skincare tracking, meditation, sex tracking, period monitoring, and more. *See* Welltory,

[4] https://www.cnn.com/2010/TECH/mobile/10/12/app.for.that/index.html.
[5] https://www.mbta.com/mbta-endorsed-apps.

Ultimate Guide to 111 Health & Wellness Apps, Medium (Dec. 20, 2017) (gathering health and wellness apps available in 2017).[6] Period-tracking apps know when and how people use contraception, when they will menstruate, and when they have sex. Mega Rajagopalan, *Period Tracker Apps Used by Millions of Women Are Sharing Incredibly Sensitive Data with Facebook*, Buzzfeed News (Sept. 9, 2019).[7] These apps also disclose this extraordinarily sensitive information to data aggregators. *Id*.

Even smartphone games collect information on media consumption and habits users would never expect. Numerous games and leisure apps collect television, advertising, and movie-viewing data. One data collection company, Alphonso, collected user data through more than 1,000 apps in 2017, including games like "Pool 3D" and "Real Bowling Strike 10 Pin." Sapna Maheshwari, *That Game on Your Phone May Be Tracking What You're Watching on TV*, N.Y. Times (Dec. 28, 2017).[8] Alphonso identifies the media playing around a user's phone from sound signals it records. *Id*.

---

[6] https://medium.com/welltory/ultimate-guide-to-111-health-wellness-apps-4d5a88010202.
[7] https://www.buzzfeednews.com/article/meghara/period-tracker-apps-facebook-maya-mia-fem.
[8] https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html.

But data collection is not limited to smartphones. Digital watches and other wearable devices that collect a wide array of personal data are worn and used every day by many individuals for fitness, productivity, and other purposes. As of June 2019, more than one-in-five Americans regularly wear a smartwatch or fitness tracking device. Emily A. Vogels, *About One-in-Five Americans Use a Smart Watch or Fitness Tracker*, Pew Res. Ctr. (Jan. 9, 2020).[9] These devices can collect a wide range of sensitive personal data including heart rate, steps, sleep patterns, and precise location. Some devices even infer or estimate medical information such as stress levels. Lisa Eadicicco, *Fitbit Just Launched a New Smartwatch that Can Tell How Stressed You Are, Beating Apple to the Punch*, Business Insider (Aug. 25, 2020).[10]

Phones and watches are not the only devices that have now become "smart." Other commonplace objects now also collect data about their users. For example, SleepNumber makes "smart beds" that collect data on a sleeper's heart rate, respiration, and movement. Julia Appleby, *Your Wake-Up Call on Data-Collecting Smart Beds and Sleep Apps*, Kaiser Health News (May 30, 2019).[11] In 2019, the

---

[9] https://www.pewresearch.org/fact-tank/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/.
[10] https://www.businessinsider.com/fitbit-sense-smartwatch-announced-stress-tracking-apple-watch-2020-8.
[11] https://khn.org/news/a-wake-up-call-on-data-collecting-smart-beds-and-sleep-apps/.

company received over 8 billion biometric data points every night from users. *Id*. Detailed data from a SleepNumber mattress could reveal a person's sleep patterns and even how often they have sex. *Id.*

Indeed, an array of traditional home appliances and other devices are now "smart" and collect personal data. There are "smart" versions of everything from thermostats to lights, speakers, ovens, refrigerators, locks, security systems, and even toys. A recent study found that 24 percent of Americans own a smart speaker device and 63 percent use a voice-operated personal assistant on their smartphone or smart speaker. *The Smart Audio Report*, National Public Radio (April 2020).[12] The share of smart speaker users with three or more devices in a home increased from one-in-five a year ago to one-in-three today. *Id.*

As shopping, work, school and other facets of daily life have moved online, there has also been a significant increase in data collection by websites. The largest internet companies, including Amazon and Google, compile detailed search and purchase histories from users, and internet service providers like Verizon and Comcast also collect browsing data. All of this data can provide a particularly personal view into an individual's thoughts, interests, and day-to-day life. Amazon's databases are not only comprehensive but historical, tracking every purchase a customer makes. Todd Haselton, *Amazon Keeps Track of Every*

[12] https://www.nationalpublicmedia.com/insights/reports/smart-audio-report/.

Purchase You've Ever Made — Here's How to See the List, CNBC (Apr. 26, 2019).[13]

Many other everyday activities are also migrating online, creating new data trails. In 2019, the share of consumers who bought groceries online jumped to a record 36.8 percent of U.S. shoppers. Coresight Research, *US Online Grocery Survey 2019* (May 14, 2019);[14] *see also* Aine Cain, *Amazon's Online Grocery Sales Tripled as People Stayed Home Amid the Coronavirus Pandemic,* Business Insider (Jul. 30, 2020).[15] Amazon's detailed purchase data has grown substantially in recent months as the pandemic has driven shoppers online—the company shipped 415 million packages in July alone. Frank Holland, *Amazon is Delivering Nearly Two-Thirds of Its Own Packages as E-commerce Continues Pandemic Boom*, CNBC (Aug. 13, 2020).[16] A single company now has records of what groceries and over-the-counter medicines consumers regularly buy, what gifts they give at the holidays, and the small purchases that get consumers through the week. A broad reading of the third-party doctrine would make all of these records available to law enforcement without a warrant or even reasonable suspicion.

---

[13] https://www.cnbc.com/2019/04/26/how-to-see-everything-youve-ever-bought-from-amazon.html.
[14] https://coresight.com/research/us-online-grocery-survey-2019/.
[15] https://www.businessinsider.com/amazons-whole-foods-grocery-sales-triple-coronavirus-pandemic-2020-7.
[16] https://www.cnbc.com/2020/08/13/amazon-is-delivering-nearly-two-thirds-of-its-own-packages.html.

Google and ISPs hold similarly sensitive databases of web searches and websites visited. Google compiles a record of every query typed into the search engine. As the intermediary between digital devices and the internet, service providers like Verizon also have detailed browsing data that is uniquely sensitive and revealing. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 Univ. Ill. L. Rev. 1418 (2009) ("An ISP can track your ailments, emotions, and the state of your relationships. It can learn your travel plans, big dates, and trips across town to do mundane chores. It can know how often you call your mother, e-mail your sister, or send gifts to your grandfather. It can know what you read, watch, buy, and borrow.").

A staggering number of companies collect granular records on users' locations to sell to data aggregators—even when that data is unnecessary to provide the service from the app. A 2018 experiment by the New York Times found that a schoolteacher's phone recorded and exported her location to a third party every two seconds. Jennifer Valentino-Devries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018).[17] Location tracking from innocuous seeming apps like AccuWeather can enable comprehensive surveillance. *See* EPIC, *EPIC v. AccuWeather* (2020).[18]

[17] https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[18] https://epic.org/privacy/litigation/consumer/epic-v-accuweather/.

Location tracking is not limited to smartphone apps. Credit card reader company Square, Inc. records the time and GPS location of each transaction, along with other information. *GPS, Maps, and Location Services*, Square (last accessed Oct. 2, 2020 at 3:11 PM).[19] Individuals are enrolled in Square's system by swiping their credit card at a terminal—and once in, it is notably difficult to de-link or remove information from their records system. Joseph Cox, *It's a Huge Pain to Get Square to Unlink Your Email From Your Credit Card*, Wired (Oct. 25, 2019).[20] With a network of phone-based card readers and recognizable white tablets, Square receives location data every time a person uses their credit card on a square terminal. Even the routine activity of swiping a card to buy a coffee can send the cardholder's time-stamped GPS location and identifying information to the company. The upshot is that revealing location to a third-party company is unavoidable when participating in public life.

B. Consumers are often unaware of data collection or do not meaningfully consent to the subsequent use or disclosure of the data for other purposes.

The mere presence of a putative choice for consumers, "hand over your data or don't use our service" is not enough to ensure that consumers have a meaningful opportunity to consent to data collection and data sharing. Consent requires a

[19] https://squareup.com/help/us/en/article/3844-gps-maps-and-location-services.
[20] https://www.vice.com/en/article/vb5jx8/how-to-delete-your-email-from-square.

knowing and voluntary agreement between parties of similar bargaining power. But terms and disclaimers buried in privacy policies that can run hundreds of pages make it essentially impossible for consumers to meaningfully review and consider the privacy practices of every firm they interact with. *See* Nancy Kim, Wrap Contracts (2013) and Neil Richards and Woodrow Hartzog, *Privacy's Trust Gap*, 126 Yale L.J. 908 (2017). The lack of meaningful consent in the digital world does not end with individual contracts. The proliferation of privacy notices has created "pathologies of digital consent" in which, across the digital landscape, consumers agree to disclose their information in situations of unwitting consent, coerced consent, and incapacitated consent. Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 94 Wash. U. L. Rev. 1461, 1478 (2019). The constant barrage of notices and consent boxes wears down consumers' abilities to meaningfully evaluate privacy policies. As Richards and Hartzog describe, "The result is a casual familiarity turned ennui that leads us to gloss over the terms because we know that another request is just around the corner. Because each consent request is a drain on our time and cognitive load, we wisely choose to conserve our efforts." *Id.* at 1493.

Reading every privacy policy is also practically impossible. According to one 2008 study, it would have taken an average consumer over 200 hours of reading a year to parse every privacy policy she is subject to online. Aleecia M.

McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S 543, 565 (2008); *see also* Yannis Bakos, Florencia Marotta-Wurgler, David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-form Contract*, 43 J. Legal Stud. 1 (2014). A study also estimated that it would take 53.8 billion hours for every internet user in the U.S. to read every privacy policy on every website they visited. *See* Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, Atlantic (Mar. 1, 2012).[21] In an art exhibition on internet surveillance, one piece entitled *How Long Does It Take to Read Amazon Kindle's Terms and Conditions?* involved an actor reading the eponymous policy. It took nine hours. Sarah Jeong, *Turning the Specter of Internet Surveillance into Art*, The Verge (Nov. 9, 2017).[22]

One journalist visually demonstrated that she could cover the length of a football field using the printed privacy policies of all apps, services, and operating systems she most regularly used. Joanna Stern, *To Read New GDPR Privacy Policies You'll Need a Football Field*, Wall Street Journal (May 18, 2018).[23]

Even Chief Justice John Roberts has admitted that even he does not read privacy policies, describing fine print-based consent models as "a problem,

---

[21] https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851.
[22] https://www.theverge.com/2017/11/9/16620452/london-glass-room-art-exhibit.
[23] https://www.youtube.com/watch?v=sucM3gKt4bE&feature=emb_logo.

because the legal system obviously is to blame for that." Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, ABA Journal (Oct. 20, 2010).[24] If some individual did take the time and energy to parse through these privacy policies, they would not likely have any better understanding of what data is being collected or how it is used. The average readability level required to understand the policies of the 500 most popular websites in the U.S. is comparable to the level for academic articles. These policies are written with language that is not accessible to the public. Uri Benoliel and Schmuel I. Becher, *The Duty to Read the Unreadable*, 60 B.C. L. Rev. 2255 (2019). It is simply not possible to accommodate the time constraints of a normal life and the time required to read, evaluate, and appropriately respond to privacy policies.

It is little surprise, then, that only 22 percent of Americans regularly read privacy policies, even though 79 percent say they are concerned with how companies use their data. Brook Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Res. Ctr. (Nov. 15, 2019) ("2019 Pew Survey").[25]As a result, most Americans—59 percent—report having very little or no understanding of what companies do with

---

24 https://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print.

25 https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

their data. *Id.* Just 6 percent of Americans feel that they understand "a great deal" of what companies do with their data. *Id*. Indeed, even the developers of apps are often unaware of what data their app collects or how it is used. Kaveh Waddell, *Some Developers Don't Know What Their Apps Do with Your Data. Here's Why.*, Consumer Reports (Mar. 13, 2020).[26] Because developers build their apps with preexisting code from other companies, even privacy-minded app developers can end up exposing their customers' information.

That data aggregators often collect individuals' data from the back end of apps casts further into question the third-party doctrine's assumption of knowing and voluntary consent. When a consumer downloads an app, they likely understand that the app's creator has at least some access to their data. However, apps do not make clear that their data is at the same time being disclosed to an aggregator operating behind the scenes. Even if an individual knowingly consents to disclose their location to SnapChat, they have no knowledge that FourSquare must also receive that data to make their app work.

Consumers' inability to fully understand when data is collected or disclosed is not a result of inadequate interest, but by design. It is often impossible to tell when data is collected, where it is going, or even to opt out. For example, apps'

[26] https://www.consumerreports.org/privacy/developers-dont-know-what-their-apps-do-with-your-data/.

location tracking settings are not always clear—and the default is often to disclose location data to the company. The popular fitness app Strava stores both real-time and historical location data from user workouts. Arielle Pardes, *How to Manage Your Privacy on Fitness Apps*, Wired (Jan. 30, 2018).[27] Under Strava's default privacy settings, this information is uploaded automatically to the company. In 2018, the Associated Press revealed that Google recorded individuals' locations even users turned off the "Location History" setting to preserve their privacy. Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, A.P. (Aug. 13, 2018).[28] Although turning off the "Location History" setting stopped Google from recording users' locations in a subsection of the Google Maps app, that setting did nothing to stop Google recording users' location through a variety of other routine cellphone tasks like performing a Google search, or even opening the Maps app. *Id*. Google is facing legal consequences for its byzantine system of location tracking settings, which make it seem to the user that they have turned off tracking when, in fact, tracking persists. *In re Google Location History Litigation*, 428 F. Supp. 3d 185 (N.D. Cal. 2020) (No. 5:18-cv-05062); *Arizona v. Google*, 2020 WL 2789903 (Ariz. Super. Ct. filed May 27, 2020); *see also* Complaint for

[27] https://www.wired.com/story/strava-privacy-settings-how-to.
[28] https://apnews.com/article/828aefab64d4411bac257a07c1af0ecb.

EPIC, *In re Google Purchase Tracking*, Fed. Trade Comm'n (July 31, 2017).[29] The same problem with deficient privacy settings made it impossible to opt out of location tracking in the AccuWeather app. *See EPIC v. AccuWeather*, No. 2018 CA 001870 B (D.C. Super. Ct. filed Mar. 16, 2018).

More broadly, it is rarely clear when and to what extent apps collect data. An individual would not reasonably expect, and would not be on notice, that playing a phone game records their media consumption preferences. Similarly, an individual could not reasonably intuit that using a weather app would record her location and send that information to a different company from the developer of the app. Even if she wanted to avoid FourSquare's location data collection, she would have to research and consciously avoid all 150,000 plus apps associated with the company. Even where that type of research is technically possible, it is too time consuming to be practical.

C. Modern privacy principles have embraced use-limitation as a fundamental aspect of privacy.

The federal government first began to develop a set of data protection rights and corresponding obligations called the Fair Information Practices ("FIPs") in the 1970s. Around the same time that the Supreme Court was creating Fourth Amendment rules for analog telephone and bank records, Congress and other

[29] https://epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf.

government entities were thinking about the broader implications of databases and computer systems for individual rights. The FIPs recognize that an individual has a right "to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent." U.S. Dep't of Health, Education, & Welfare, *Records, Computers and the Rights of Citizens* (1973).[30] This use limitation right has been implemented in several major federal privacy statutes, including the Privacy Act of 1974, 5 U.S.C. § 552a(e) and the Cable Communications Policy Act of 1984, 47 U.S.C. § 551.

The use limitation right continues to underpin privacy law both domestically and abroad. The right lies at the core of the California Consumer Privacy Act (CCPA), mandating use limitation and requiring businesses to allow customers to opt-out of data sales to third parties. Cal. Code § 1798.100(b) (West 2020) ("A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section."). Article 5 of the

[30] https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.

European Union's General Data Protection Regulation (GDPR) also mandates that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." 2016 O.J. 119 (Art. 5 § 1(b)).

Use limitation conforms to the public's expectations of how their data should be used. In a 2015 report, Pew found that 93 percent of adults want control over who can access their information, with 74 percent considering that control "very important." Mary Madden and Lee Raine, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Res. Ctr. (May 20, 2015).[31]

III. This Court should reject the third-party doctrine for electronic data collected by a third party from an individual for the purpose of obtaining a service.

Data-driven technologies have become essential to modern life in ways patently unimaginable mere decades ago. Individuals regularly have no choice but to mediate their daily activities through third parties when they pay for groceries, sleep on their mattresses, go for a run, or ride the Red Line. Today's technological landscape is a dramatic departure from that of the 1970s, when the third-party doctrine aligned with the way companies collected data from consumers—in a limited, service-based fashion. Instead, consumers now navigate a society in which

[31] https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

data is constantly gathered as they go about their daily lives, often without an opportunity to meaningfully consent. Consumers can no longer access basic services without being forced to disclose large amounts of personal data. They have no control over how much of it and to whom their data is disclosed. The third-party doctrine is "ill suited to the digital age" in which consumer consent is not limited to the purpose for which data is collected but rather extends as far as government interests may dictate. *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring). By allowing law enforcement to access data without a warrant, the third-party doctrine violates the fundamental right to privacy.

This Court should reject the third-party doctrine for electronic data obtained by third parties that provide a particular service to consumers. Instead, the court can more accurately address issues of consent and societal expectations of privacy through the principle of use limitation. Where consumers turn over data to a company in the process of obtaining a service, they do not lose all expectation of privacy in their data. The use limitation principle reflects this fact because it requires third parties to obtain consent to collect and disclose data for additional purposes when a consumer initially provides data for a particular purpose. Unlike the third-party doctrine, this principle is not a relic of a bygone era before modern computers and databases became widespread; the FIPs have developed with the shift to a data-centric world and have been applied globally in modern privacy

laws. As new technologies emerge, data collection practices will only intensify. This court should align its reasonable expectation of privacy analysis with societal expectations and modern privacy law by rejecting the third-party doctrine.

This court recognized in *Augustine* that the invasive nature of a particular technology and its prevalence in society can implicate the constitutionally-protected interest in a reasonable expectation of privacy. Many new technologies that have become a necessary element of modern life produce troves of personal data on each user as they go about their day. Many services use predictive analytics to compile detailed profiles on individuals and these data systems are built in to many services that we use every day. Seemingly quotidian activities like checking your bank account and commuting to work are instantly "datafied," or translated into data, so that third parties can track and optimize their services.

Although people today "reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," they largely do so "for a limited purpose." *Jones*, 565 U.S. at 417. The third-party doctrine is "inapposite" to an age which has "altered dramatically the societal landscape from the 1970s" because it rests on an outdated principle: By disclosing information with a company for a particular purpose, a consumer is not actively assuming the risk that the company could disclose that exact information to the government. *Augustine*, 467 Mass. 230, 245 (2014). As with CSLI, most third-party data is not

voluntarily conveyed by the consumer but is "purely a function and product" of the way third parties operate their services; it is "created by the provider's system network at the time" that a consumer uses an application. *Id.* at 250. The data collected by businesses today is not a limited set of information like the call details in *Smith* or the deposit slip in *Miller*; these databases contain huge volumes of incredibly sensitive and revealing personal data. What is true for CSLI is just as true for other forms of third party data, namely that "it is of course the case that [such data] has no connection at all to the reason people use" these technologies. *Id.*

Third parties regularly collect revealing personal data on consumers' bodies, in their homes, and on their internet browsers. Numerous companies collect biometric information through smart devices and Internet-of-Things connected products. Major e-commerce companies hold detailed purchase histories which can reveal intimate aspects of a life. Internet search histories hold the potential to reveal a person's thoughts and private activities. This data can be incredibly sensitive and would be otherwise unknowable with such precision—every online purchase in the past three years, every pillow talk session with a partner, every increased heartrate and where one was when it happened. The data is "unknown and unknowable to the [third party] user in advance—or probably at any time until he or she receives a copy of the [data] itself." *Augustine*, 467 Mass. at 250.

Third party data can thus form a revealing mosaic in which location data is just one type of tile. Law enforcement investigations increasingly seek this data because it is so precise, detailing a suspect's behaviors and past actions mechanically, efficiently, and without the need to expend department resources. *See* Gilad Edelman, *Can the Government Buy Its Way Around the Fourth Amendment?*, Wired (Feb. 11, 2020) (describing how DHS buys location data directly from a data aggregator instead of seeking subpoenas).[32] Police in a prior era would have absolutely no means of obtaining the information contained within a single health and wellness app today.

The third-party doctrine allows the government to access all of this data without a warrant, undermining citizens' reasonable expectations that their personal data will only be collected, used, and disclosed specified purposes. *See Jones*, 566 U.S. at 413-418 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

As ever more services are mediated through third party technologies, the third-party doctrine erodes societal expectations of privacy as a condition of

[32] https://www.wired.com/story/can-government-buy-way-around-fourth-amendment.

participating in modern life. Without meaningful limits on government access to data, the potential for police to obtain personal information on all aspects of private life will continue to expand.

The main benefit of the third-party doctrine was its simplicity. But an equally simple rule would provide much needed privacy protection in the digital age. Electronic data collected for the purpose of obtaining a service should not be disclosed for law enforcement purposes without a warrant. This use limitation rule would be more consistent with individual expectations and the underlying purpose of constitutional privacy protections. If the Court does not adopt such a rule, it will be repeatedly tasked with deciding whether an individual has a reasonable expectation of privacy in every new type of digital data. Both this court and the Supreme Court have already spent years considering any possible differences between location data obtained from a GPS tracker and location data obtained from a cell phone provider. But, as Section II.A. demonstrates, companies and service providers now routinely collect huge volumes of much more sensitive and invasive data. Relying on idiosyncratic rules about each type of sensitive data will not scale. Constitutional privacy protections require brighter lines than that.

Luckily, the expectations of individuals are not based on the unique factors of different data types or services. The core assumption about data collection systems under modern privacy regimes is that when an entity collects data to

provide a particular service, that data will not be used or disclosed for other purposes without the individual's consent. This aligns exactly with the principle of use limitation. Further data collection and sharing with other entities requires additional consumer consent by various laws, including the CCPA and GDPR. By failing to account for use limitation, the third-party doctrine of *Smith* and *Miller* has fallen far behind modern privacy practices.

The present case provides an excellent opportunity for the court to reject the third-party doctrine and rely instead on the use limitation principle. The Charlie Card is an example of a basic service on the precipice of its own digital revolution. The court today considers Charlie Card data that is limited to a serial number providing point-of-entry information to the transit system for fare purposes. While the data collected by the third party in this case seems limited now, the data collected by the system will necessarily expand over time. In 2017, the MBTA contracted with a global provider of contactless fare collection systems to transition to a contactless transit system. *See Goodbye, CharlieCard: MBTA Approves $723M to Modernize Fare Collection*, Boston 25 News (Nov. 24, 2017).[33] Contactless fare collection systems enable riders to ditch a physical transit card and instead use tap payment turnstiles with their credit/debit cards and

[33] https://www.boston25news.com/news/goodbye-charliecard-mbta-proposes-723m-overhaul-of-fare-system/650689473.

smartphone payment apps. *See* Ali Winston, *The NYC Subway's New Tap-to-Pay System has a Hidden Cost—Rider Data*, The Verge (Mar. 16, 2020).[34] These systems link riders' movements on public transit directly to their bank card and, more alarmingly, to the various kinds of data captured regularly by smartphones. This data is collected not by the MBTA, but by the third-party company maintaining the contactless system's servers. *Id.*

If this court applies the third-party doctrine to Charlie Card data today, it will compromise privacy in the wide array of data that third parties will collect from every transit user when they tap their smartphone at a contactless turnstile. The police would be able to access this data without a warrant simply because a suspect used public transit and, due to the transition to contactless fare collection, had no choice but to use their smartphone to board the train. The Court should not take that route. Instead, the Court should replace the third-party doctrine with a constitutional jurisprudence that can adapt to new technologies. The Court should hold that an individual's reasonable expectation of privacy is violated when their data is used or disclosed beyond to the primary purpose for which they provided it. If the government seeks to access to Charlie Card data for investigative purposes, it must do so with a warrant.

[34] https://www.theverge.com/2020/3/16/21175699/mta-omny-privacy-security-smartphone-identifier-location-nyc.

CONCLUSION

Amicus respectfully requests that this Court retire the third-party doctrine in this and all future cases involving electronic data collected by third parties. As society evolves with the times, so too must the law.

Respectfully submitted,

*/s/ Caitriona Fitzgerald*_____
Caitriona Fitzgerald
Counsel of Record
Alan Butler
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

CERTIFICATE OF COMPLIANCE

I hereby certify that the above brief complies with the rules of court that pertain to the filing of brief, including, but not limited to: Rule 16(a)(13); Rule 16(e); Rule 18; Rule 20; and Rule 21. This brief complies with the type-volume limitation of Rule 20(2)(C) because it contains 7,172 words, excluding the parts of the brief limited by the rule. It complies with the type style requirements of Rule 20 because it has been prepared in proportionally spaced typeface using Microsoft Office Word in 14-point Times New Roman style.

Dated: October 16, 2020

*/s/ Caitriona Fitzgerald*_____
Caitriona Fitzgerald
Counsel of Record
Alan Butler
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

CERTIFICATE OF SERVICE

Pursuant to Massachusetts Appellate Rule of Procedure 13(c), I hereby certify that on October 16, 2020, this brief was electronically filed with the Clerk of the Court for the Supreme Judicial Court. I have made service of this Brief upon the attorney of record for each party by Electronic Filing System.

Dated: October 16, 2020

*/s/ Caitriona Fitzgerald*_____
Caitriona Fitzgerald
Counsel of Record
Alan Butler
Megan Iorio
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140